

On Ideal Lattices over the Tensor Product of Number Fields and Ring Learning with Errors over Multivariate Rings

Alberto Pedrouzo-Ulloa* Juan Ramón Troncoso-Pastoriza*
 Fernando Pérez-González*

July 19, 2016

Abstract

The “Ring Learning with Errors” (RLWE) problem was formulated as a variant of the “Learning with Errors” (LWE) problem, with the purpose of taking advantage of an additional algebraic structure in the underlying considered lattices; this enables improvements on the efficiency and cipher expansion on those cryptographic applications which were previously based on the LWE problem. In Eurocrypt 2010, Lyubashevsky *et al.* introduced this hardness problem and showed its relation to some known hardness problems over lattices with a special structure. In this work, we generalize the results and the hardness problems presented by Lyubashevsky *et al.* to the more general case of multivariate rings, highlighting the main differences with respect to the security proof for the RLWE counterpart. We denote this hardness problem as “Multivariate Ring Learning with Errors” (m -RLWE or multivariate RLWE) and we show its relation to hardness problems over the tensor product of ideal lattices. Additionally, the m -RLWE problem is more adequate than its univariate version for cryptographic applications dealing with multidimensional structures.

Keywords Tensor Number Fields, Lattice Cryptography, Ring Learning with Errors, Multivariate Rings, Hardness Problems.

1 Introduction

In recent years, a high number of cryptographic schemes and applications have been proposed based on the LWE (Learning with Errors) problem. However, in spite of the versatility of this hardness assumption for developing cryptographic primitives, the main drawback of the cryptosystems whose security is based on LWE is their efficiency. Actually, several schemes that allow to perform an unbounded number of encrypted operations (Fully Homomorphic Encryption Schemes, FHE) have been devised, but the needed size of the keys and the required computation times are still too high for practical applications.

In order to alleviate this issue, an algebraic version of the LWE problem was proposed by Lyubashevsky *et al.* [15, 14]. This hardness assumption, called ring-LWE, is based on worst-case problems on ideal lattices instead of general lattices. Although the use of lattices with an additional algebraic structure could allow for the existence of better

*Signal Theory and Communications Department, University of Vigo, 36310 Vigo, Spain (apedrouzo@gts.uvigo.es, troncoso@gts.uvigo.es, fperez@gts.uvigo.es).

attacks, nowadays there are no known attacks to RLWE that get a substantial advantage with respect to attacks to LWE.¹

Hence, the RLWE problem and the analysis of its security reductions to hardness problems on ideal lattices have enabled the introduction of new cryptographic applications: Brakerski *et al.* [8, 7] proposed several versions of FHE cryptosystems, varying from leveled FHE schemes to the most recent scale-invariant versions [10, 6, 5].

Practical applications in the field of Secure Signal Processing (SSP) have made extensive use of homomorphic encryption [3], and especially additive schemes like Paillier’s [20]. However, the Paillier cryptosystem has several drawbacks for practical implementations, being its two main problems the very high cipher expansion and the inability to perform multiplications between two encrypted messages.

In order to resolve the first drawback, packing and unpacking steps were introduced in [27, 4]; for the second drawback, several recent works resort to Somewhat Homomorphic Encryption (SHE) schemes [26] to enable simultaneous use of fully encrypted signals. While SHE schemes only allow for a limited number of encrypted operations, they are more efficient than their Fully Homomorphic counterparts. Therefore, if the number of operations that have to be performed under encryption is known beforehand (this is usually true in many practical applications), the use of SHE schemes increases the efficiency of the solution.

Nevertheless, when working with multidimensional signals, both the Paillier cryptosystem and the RLWE based cryptosystems present a very high cipher expansion (even after incorporating packing and unpacking techniques). In this context, the authors [21] introduced some example cryptosystems based on a variant of the RLWE problem called m -RLWE (multivariate Ring Learning with Errors) that extends RLWE from the univariate case to the multivariate one. These cryptosystems can be defined by extending to the multivariate case the most typical RLWE based cryptosystems. They bring about clear advantages in terms of efficiency and size of the underlying lattice when working with multidimensional signals, and they allow for packing several signals in only one ciphertext. It is also important to note that some of the contributions of [21] can be adapted to work with RLWE based cryptosystems considering the tensorial decomposition in “co-prime” cyclotomic fields shown in the work of Lyubashevsky *et al.* [16]. This approach only requires to have enough space inside the polynomials in order to properly store the result of linear convolutions.

However, there are several applications that cannot be easily adapted to the RLWE case, like those presented in [22], because a particular modular function is needed to enable several usual operations belonging to the field of Signal Processing. In addition, having the same modular function on several variables can be a requirement in some cases, and this is not considered in the work of Lyubashevsky *et al.* and can only be tackled by resorting to the m -RLWE problem.

While several comparisons between m -RLWE and RLWE have been presented considering basis-reduction attacks [9, 18] and decoding attacks as described in [13], a reduction to hardness problems on lattices and a complete security proof have not been provided yet; this is the main contribution of this work.

Therefore, the main objective of this work is to adapt and generalize the techniques of Lyubashevsky *et al.* [14] for the RLWE problem and achieve a reduction of the m -RLWE to hardness problems over ideal lattices, hence proving the security of the m -RLWE prob-

¹In [17], Albrecht *et al.* take advantage of the presence of a subfield in the considered number field which allows them to deal with an easier lattice problem. However, while this technique allows to have an attack for the overstretched NTRU problem, the RLWE problem is not affected.

lem. For the sake of simplicity, we present a generalized version of the multivariate RLWE problem introduced on [21] that is limited to only work with cyclotomic modular functions of degree power of two, but it is possible to have any type of cyclotomic polynomial as modular function.

1.1 Structure and notation

The structure of the paper is as follows: Section 2 extends some properties of cyclotomic number fields to the tensor product case. Section 3 introduces the m -RLWE problem together with the main theorem and the necessary definitions. Finally, Section 4 presents the security reductions for m -RLWE along with the involved theorems, sketching their proof. Appendix A revisits the necessary concepts of algebraic number theory and lattices when they are extended to the tensor of number fields, while Appendices B and C present the lemmas and proofs for the main reductions.

We denote matrices and vectors with uppercase and lowercase letters, respectively; $\langle \mathbf{a}, \mathbf{b} \rangle$ represents the scalar product between two vectors \mathbf{a} and \mathbf{b} . For a vector $\mathbf{x} \in \mathbb{C}^n$ we define its l_p norm as $\|\mathbf{x}\|_p = \left(\sum_{i \in [n]} |x_i|^p \right)^{1/p}$, where $1 \leq p < \infty$ with $p \in \mathbb{R}$, and $\|\mathbf{x}\|_\infty = \max_{i \in [n]} |x_i|$. If p is omitted, we consider the Euclidean norm.

The set $[n]$ is defined as $\{1, 2, \dots, n\}$. We also work with some additional operators as the tensor product \otimes and the direct sum \oplus . When dealing with number fields (or the corresponding ring of integers), as the tensor product is always defined over the rational numbers (integer numbers) we ignore the subscript if there is no ambiguity.

2 Properties of the Tensor Product of Cyclotomic Number Fields

For the sake of completeness, we discuss why the embeddings, automorphisms and even the Chinese Remainder Theorem (CRT, see Appendix A.3.8) can be perfectly defined over the tensor of cyclotomic fields and the corresponding tensor ring of integers. Although the three previous concepts are interrelated, we separately explain their existence in the following sections.

The notation and tools used throughout this discussion are defined in Appendix A, which introduces the main concepts needed to obtain the security proofs of the multivariate extension of the RLWE problem, by extending several of the concepts presented in [14] to our more general case. We refer to this appendix when needed, but we encourage the reader to go over it before reading this section.

2.1 Embeddings

We can work with the embedding over the space H (see Appendix A.1) of any type of cyclotomic field. Of course, as we can decompose a cyclotomic field in the tensor of power prime cyclotomic fields, it is easily shown that for that particular case of tensor of cyclotomic fields the embedding exists.

However, in our more general case this relation with cyclotomic fields does not necessarily hold, so we can not justify the existence of the tensor embedding by solely resorting to the existence of the embedding in an isomorphic cyclotomic field.

We can see that the embedding of a cyclotomic field (respectively, its corresponding ring of integers or the corresponding reduction modulo q) is equivalent to an invertible

linear transformation from $\mathbb{Q}^{\phi(m_i)}$ (respectively, $\mathbb{Z}^{\phi(m_i)}$ or $\mathbb{Z}_q^{\phi(m_i)}$) to the corresponding subspace $H_i \subseteq \mathbb{C}^{n_i}$, where $n_i = \phi(m_i)$ (see Appendix A).

Now, there are two properties of Kronecker products that allow us to justify the existence of the embeddings. The first one is that

$$\det(\mathbf{A} \otimes \mathbf{B}) = \det(\mathbf{B} \otimes \mathbf{A}) = (\det(\mathbf{A}))^n (\det(\mathbf{B}))^m,$$

where \mathbf{A} and \mathbf{B} are square matrices of size $n \times n$ and $m \times m$, respectively. This property states that $\mathbf{A} \otimes \mathbf{B}$ is non singular (and therefore invertible) if and only if \mathbf{A} and \mathbf{B} are non singular. The second one is that $(\mathbf{A} \otimes \mathbf{B})^{-1} = \mathbf{A}^{-1} \otimes \mathbf{B}^{-1}$, which defines this inverse. For more details about the different properties of the Kronecker product we refer the reader to [11].

Additionally, we can see that our embedding can be defined as the Kronecker product of different invertible linear transformations that correspond to the different embeddings for each cyclotomic field. Hence, resorting to the properties of the Kronecker product we can see that there exists the corresponding tensor embedding between the tensor of cyclotomic fields and the subspace $H(T) = \bigotimes_{i \in [l]} H_i$ (see Appendix A.1).

2.2 Automorphisms and Linear Representation Theory

In order to justify the structure and behaviour of the new automorphisms we resort to the theory of Linear Representations [25]. First, we introduce the main concepts needed from this theory, and afterwards, we detail the different automorphisms that we can find.

In general, we consider V as a vector space of dimension d over \mathbb{C} and we define $\text{GL}(V)$ as the group composed of all the isomorphisms of V onto itself. An element a belonging to $\text{GL}(V)$ can be seen as a linear mapping from V to V and we denote its inverse as a^{-1} . Analogously, we could think of each linear mapping as an invertible square matrix A of size $d \times d$ whose coefficients are complex numbers. Hence, we can see that $\text{GL}(V)$ is composed of all the different invertible square matrices of order d .

Now, if we consider a finite group G , we define a linear representation of G in V as a homomorphism ρ from G to $\text{GL}(V)$. Considering that the group G has the composition operation $(r, s) \rightarrow rs$ for $r, s \in G$, we have the following property:

$$\rho(rs) = \rho(s)\rho(r),$$

where $\rho(r)\rho(s)$ represents the matrix multiplication operation between the two associated matrices to r and s , respectively. Two important properties are that when $1 \in G$, this implies $\rho(1) = 1$ and $\rho(s^{-1}) = \rho(s)^{-1}$. Commonly, we consider V as a representation space (or simply a representation) of G .

Now, we can particularize the previous results to our specific case, for $W = \mathbb{Q}(\zeta_{m_i}) \subset \mathbb{C}$ (see Appendix A.3). If we consider $G = \mathbb{Z}_{m_i}^*$ and as the composition operation we consider the product operation between units of \mathbb{Z}_{m_i} , we have the following linear representation $\rho_i : \mathbb{Z}_{m_i}^* \rightarrow \text{GL}(\mathbb{Q}(\zeta_{m_i}))$ where $\rho_i(\mathbb{Z}_{m_i}^*) \subseteq \text{GL}(\mathbb{Q}(\zeta_{m_i}))$ is composed of the different automorphisms $\tau_k = \rho_i(k)$ for $k \in \mathbb{Z}_{m_i}^*$ such that $\tau_k(\zeta_{m_i}) = \zeta_{m_i}^k$, hence having $\mathbb{Q}(\zeta_{m_i})$ as a representation of $\mathbb{Z}_{m_i}^*$. It is important to note that the effect of the automorphism τ_k over the embedding is a rotation of the coordinates of the subspace H_i , that is, $\sigma_i(\tau_k(\zeta_{m_i})) = \sigma_{ik}(\zeta_{m_i})$, being $i \in \mathbb{Z}_{m_i}^*$.

Of course, the linear representation preserves the linear structure and, in this case, as we have a commutative group $\mathbb{Z}_{m_i}^*$, there exists an equivalent representation such that each square matrix associated to each particular automorphism can be decomposed as a

direct sum of n irreducible representations $\bigoplus_{j \in [n_i]} V_j$ (i.e., each irreducible representation for which the only decomposition is the trivial one $V_j = 0 \oplus V_j$). This implies that there exists an isomorphic domain where we can represent all the elements of K_i in such a way that each different representation (different automorphism of K_i) of $\mathbb{Z}_{m_i}^*$ can be applied as an element-wise product over this isomorphic domain, and each different component represents a different irreducible subrepresentation of V .

Outer tensor product of Linear Representations Let two groups (G_1, \cdot) and (G_2, \cdot) and consider the direct product $G_1 \times G_2$ with the considered “ \cdot ” operation: $(s_1, s_2) \cdot (t_1, t_2) = (s_1 \cdot s_2, t_1 \cdot t_2)$ where $(s_1, s_2), (t_1, t_2) \in G_1 \times G_2$.

If we now define $\rho^1 : G_1 \rightarrow \text{GL}(V_1)$ and $\rho^2 : G_2 \rightarrow \text{GL}(V_2)$ as linear representations of G_1 and G_2 , we can now define a linear representation $\rho^1 \otimes \rho^2 : G_1 \times G_2 \rightarrow \text{GL}(V_1 \otimes V_2)$ by setting:

$$(\rho^1 \otimes \rho^2)(s_1, s_2) = \rho^1(s_1) \otimes \rho^2(s_2).$$

This way of dealing with the tensor of different linear representations allows us to define the different automorphisms of the tensor field $K_{(T)} = \bigotimes_{i \in [l]} K_i$ in terms of the automorphisms of each K_i . Then, we have for $K_{(T)}$ the corresponding homomorphism with the tensor of linear representations $\bigotimes_{i \in [l]} \rho_i : \bigoplus_{i \in [l]} \mathbb{Z}_{m_i}^* \rightarrow \text{GL}\left(\bigotimes_{i \in [l]} \mathbb{Q}(\varsigma_{m_i})\right)$, and where each ρ_i satisfies $\rho_i(k_i) = \tau_{k_i}^{(i)}$, with $k_i \in \mathbb{Z}_{m_i}^*$ and being $\tau_{k_i}^{(i)}$ the corresponding $\phi(m_i)$ automorphisms of the K_i number field.

Finally, in order to map the set of $\prod_{i \in [l]} \phi(m_i)$ automorphisms $\bigotimes_{i \in [l]} \tau_{k_i}^{(i)}$ with only one index we can consider the relation given in Equation (3) (Appendix A.1), in such a way that $k_i \in \mathbb{Z}_{m_i}^* = g^{(i)}([\phi(m_i)])$ and $j_i = g^{(i)}(k_i)$.

2.3 Chinese Remainder Theorem

In this section we explain why the CRT works over multivariate polynomial rings and how the use of the previously presented automorphisms affects the decomposition caused by the CRT.

First, consider $R = \mathcal{O}_{K_i} = \mathbb{Z}[\varsigma_{m_i}]$, the ring of integers of a number field $\mathbb{Q}(\varsigma_{m_i})$ where ς_{m_i} is the m_i -th primitive root of unity. We know that if we work with the ideal $\langle q \rangle = qR$ and $q \in \mathbb{Z}$ is a prime, we have the following factorization $\langle q \rangle = \prod_i \mathfrak{q}_i^e$ where there are $\phi(m_i)/(ef)$ different \mathfrak{q}_i of norm q^f and we have $e = \phi(q')$ and f is the minimum natural number that satisfies $q^f \equiv 1 \pmod{m_i/q'}$ with q' the largest power of q that divides m_i .

For each ideal, we have $\mathfrak{q}_j = \langle q, F_j(\varsigma_{m_i}) \rangle$ with $\Phi_{m_i}(x) = \prod_j (F_j(x))^e$ being the factorization of $\Phi_{m_i}(x)$ modulo q . As explained in [14], when we consider that $q \equiv 1 \pmod{m_i}$, both e and f are equal to 1 and as we have an m_i -th primitive root of unity w_i in \mathbb{Z}_q we see that $\Phi_{m_i}(x) = \prod_{j \in \mathbb{Z}_{m_i}^*} (x - w_i^j)$. Therefore, we finally have $\langle q \rangle = \prod_{j \in \mathbb{Z}_{m_i}^*} \mathfrak{q}_j$ with $\mathfrak{q}_j = \langle q, \varsigma_{m_i} - w_i^j \rangle$. In addition, we know that we can use the automorphism $\tau_k^{(i)}$ to exchange the contents between two different prime ideals \mathfrak{q}_j of qR , that is, we can do $\tau_k^{(i)}(\mathfrak{q}_j) = \mathfrak{q}_{j/k}$ (see Lemma 2.16 in [14]).

Now, resorting to Lemma 9 in Appendix A.3.8, we have an isomorphism from $\mathbb{Z}[\varsigma_{m_i}]/\langle q \rangle$ to $\bigoplus_{j \in \mathbb{Z}_{m_i}^*} \mathbb{Z}[\varsigma_{m_i}]/\langle q, \varsigma_{m_i} - w_i^j \rangle$, that is in fact also isomorphic to $\mathbb{Z}_q^{\phi(m_i)}$.

Multivariate extension We can see the multivariate case $R = \bigotimes_{i \in [l]} \mathcal{O}_{K_i}$ as the tensor product between the previously considered univariate rings, that is, we have $\bigotimes_{i \in [l]} \mathbb{Z}[\varsigma_{m_i}]/\langle q \rangle$ where q has to satisfy $q \equiv 1 \pmod{m_i}$ for all $i \in [l]$. Now, we know

that it is isomorphic to the tensor product of the respective direct sum in terms of the different prime ideals $\bigotimes_{i \in [l]} \left(\bigoplus_{j \in \mathbb{Z}_{m_i}^*} \mathbb{Z}[\varsigma_{m_i}] / \langle q, \varsigma_{m_i} - w_i^j \rangle \right)$ where we know that the tensor and direct product commute, therefore having

$$\bigoplus_{j \in [\prod_{i \in [l]} \phi(m_i)]} \left(\bigotimes_{k \in [l]} \mathbb{Z}[\varsigma_{m_k}] / \langle q, \varsigma_{m_k} - w_k^{j_k} \rangle \right),$$

where the mapping between the set $\{j_1, \dots, j_l\}$ and j is defined by Equation (3). This ring is in fact isomorphic to $\mathbb{Z}_q^{\prod_{i \in [l]} \phi(m_i)}$.

Resorting to the ring isomorphism $\varsigma_{m_i} \rightarrow x_i$ for $i \in [l]$ we have the expression $\bigoplus_{i \in [l], j_i \in \mathbb{Z}_{m_i}^*} \mathbb{Z}_q[x_1, \dots, x_l] / \langle x_1 - w_1^{j_1}, \dots, x_l - w_l^{j_l} \rangle$. Now, thanks to the mapping introduced in Equation (3), we consider $\mathfrak{q}_j = \mathfrak{q}_{j_1, \dots, j_l} = \langle x_1 - w_1^{j_1}, \dots, x_l - w_l^{j_l} \rangle$ with $j \in [\prod_{i \in [l]} \phi(m_i)]$. First, it can be easily shown that each \mathfrak{q}_j is an ideal and, as there is an isomorphism from $\mathbb{Z}_q[x_1, \dots, x_l] / \mathfrak{q}_j$ to the finite field \mathbb{Z}_q , \mathfrak{q}_j is a maximal ideal and also a prime ideal because every maximal ideal over a ring is also a prime ideal.

In order to show that all the \mathfrak{q}_j are comaximal ideals we have the following *reductio ad absurdum* argument: consider two different maximal ideals \mathfrak{q}_j and \mathfrak{q}_k with $k \neq j$; by definition, $\mathfrak{q}_k + \mathfrak{q}_j$ is also an ideal; we have three possible cases: a) $\mathfrak{q}_k + \mathfrak{q}_j = \mathfrak{q}_k$, b) $\mathfrak{q}_k + \mathfrak{q}_j = \mathfrak{q}_j$ and c) there is another maximal ideal $\mathfrak{q}_k + \mathfrak{q}_j$. The first two cases are not true because \mathfrak{q}_k and \mathfrak{q}_j are different, and the third case is impossible because each ideal is maximal, hence having $\mathfrak{q}_k + \mathfrak{q}_j = \mathbb{Z}_q[x_1, \dots, x_l]$, which is the definition of comaximal ideals.

Then, knowing that we have a set of comaximal ideals \mathfrak{q}_j for $j \in [\prod_{i \in [l]} \phi(m_i)]$, we can use Lemma 9 in Appendix A.3.8 to show that there exists an isomorphism from $\mathbb{Z}_q[x_1, \dots, x_l] / \langle \Phi_{m_1}(x_1), \dots, \Phi_{m_l}(x_l) \rangle$ to $\bigoplus_{j \in [\prod_{i \in [l]} \phi(m_i)]} (\mathbb{Z}_q[x_1, \dots, x_l] / \mathfrak{q}_j)$, that is, we can compute the corresponding CRT, and the rest of the properties discussed in Appendix A.3.8 also apply.

Now, we can present a similar result to Lemma 2.16 in [14], but adapted to our more general case:

Lemma 1 (Lyubashevsky *et al.* [14] Lemma 2.16). *For any $\mathfrak{q}_j = \mathfrak{q}_{j_1, \dots, j_l}$ and $\mathfrak{q}_{j'} = \mathfrak{q}_{j'_1, \dots, j'_l}$ (by Equation (3)), we have a linear representation or automorphism $\bigotimes_{i \in [l]} \rho_i(k_1, \dots, k_l) = \bigotimes_{i \in [l]} \tau_{k_i}^{(i)}$ where $k_i \in \mathbb{Z}_{m_i}^*$ satisfies $\bigotimes_{i \in [l]} \tau_{k_i}^{(i)}(\mathfrak{q}_j) = \mathfrak{q}_{j'}$.*

3 multivariate Ring-LWE

We define the multivariate RLWE distribution as a generalization of the RLWE distribution where the involved polynomial rings can have several indeterminates. The m -RLWE distribution is parameterized by a tensor number field $K_{(T)} = \bigotimes_{i \in [l]} K_i$ where each K_i is a cyclotomic number field; not necessarily being all of them different. We also consider the ring R as the tensor of the corresponding ring of integers \mathcal{O}_{K_i} , that is, $R = \bigotimes_{i \in [l]} \mathcal{O}_{K_i}$ and an integer modulus $q \geq 2$. We denote \mathcal{J}_q for $\mathcal{J}/q\mathcal{J}$ where \mathcal{J} is a fractional ideal in $K_{(T)}$. Let R^\vee be the dual fractional ideal of R and $\mathbb{T} = K_{(T), \mathbb{R}} / R^\vee$.²

Definition 1 (Multivariate ring LWE distribution). *For $s \in R_q^\vee$ and an error distribution ψ over $K_{(T), \mathbb{R}}$, a sample from the m -RLWE distribution $A_{s, \psi}$ over $R_q \times \mathbb{T}$ is generated by $a \leftarrow R_q$ uniformly at random, $e \leftarrow \psi$, and outputting $(a, b = (a \cdot s)/q + e \bmod R^\vee)$.*

² $K_{(T), \mathbb{R}}$ is defined as $K_{(T)} \otimes_{\mathbb{Q}} \mathbb{R}$. For more details we refer the reader to Appendix A.3.2.

Definition 2 (Multivariate ring LWE, Search). *Let Ψ be a family of distributions over $K_{(T),\mathbb{R}}$. m -RLWE $_{q,\Psi}$ denotes the search version of the m -RLWE problem. It is defined as follows: given access to arbitrarily many independent samples from $A_{s,\Psi}$ for some arbitrary $s \in R_q^\vee$ and $\psi \in \Psi$, find s .*

Next, we include the decision version of the m -RLWE problem:

Definition 3 (Multivariate ring LWE, Average-Case Decision). *Let Υ be a distribution over a family of error distributions, each over $K_{(T),\mathbb{R}}$. The average-case decision version of the m -RLWE problem, denoted m -R-DLWE $_{q,\Upsilon}$, is to distinguish with nonnegligible advantage between arbitrarily many independent samples from $A_{s,\psi}$, for a random choice of $(s, \psi) \leftarrow U(R_q^\vee) \times \Upsilon$,³ and the same number of uniformly random and independent samples from $R_q \times \mathbb{T}$.*

For an asymptotic treatment of the m -RLWE problems, we let $K_{(T)}$ come from an infinite sequence of tensor number fields $\mathbb{K} = \{K_{(T),n}\}$ of increasing dimension n (n is the number of basis elements that form the integral basis), and let q , Ψ , and Υ depend on n as well.

Error distributions We include here two definitions about the error distributions to achieve the reductions for the search version of multivariate ring-LWE (Definition 4) and for the hardness result for the average-case decision problem (Definition 5). We refer the reader to Appendices A.2 and A.3.2 for further information about Gaussian distributions over a tensor field.

Definition 4 (extension of Lyubashevsky *et al.* [14], Definition 3.4). *For a positive real $\alpha > 0$, the family $\Psi_{\leq \alpha}$ is the set of all elliptical Gaussian distributions $D_{\mathbf{r}}$ (over $K_{(T),\mathbb{R}}$) where each parameter $r_i \leq \alpha$ with $i \in [n]$.*

Definition 5 (extension of Lyubashevsky *et al.* [14], Definition 3.5). *Let $K_{(T)} = \bigotimes_{i \in [l]} K_i$ where the K_i are the m_i -th cyclotomic number field having degree $n_i = \phi(m_i)$. For a positive real $\alpha > 0$, a distribution sampled from Υ_α is given by an elliptical Gaussian distribution $D_{\mathbf{r}}$ (over $K_{(T),\mathbb{R}}$) whose parameters are $r_{i,j} = r_{i,j+n_i/2}$ (see Appendix A.2) and each r_j with $j \in [n]$ satisfies $r_j^2 = \alpha^2(1 + \sqrt{n}x_j)$, where whenever we have r_i and r_j such that $i, j \in [n]$, $i \neq j$, the corresponding x_i and x_j are chosen independently from the distribution $\Gamma(2, 1)$.*

Our *main theorem* is obtained by combining the theorems from Sections 4.1 and 4.2 (see Appendix A.3.7 for the definitions of lattice hardness problems; i.e., SVP and SIVP):

Theorem 1 (Extended version to m -RLWE of Lyubashevsky *et al.* [14] Theorem 3.6). *Let $K_{(T)} = \bigotimes_{i \in [l]} K_i$ be the tensor product of l cyclotomic fields of dimension $n_i = \phi(m_i)$ each, and $R = \bigotimes_{i \in [l]} \mathcal{O}_{K_i}$ the tensor of their corresponding ring of integers. Let $\alpha < \sqrt{\log n/n}$, and let $q = q(n) \geq 2$, $q \equiv 1 \pmod{m_i}$, for all i , be a $\text{poly}(n)$ -bounded prime such that $\alpha q \geq \omega(\sqrt{\log n})$, where $\omega(f(n))$ denotes a function that asymptotically grows faster than $f(n)$. Then, there is a polynomial-time quantum reduction from $\tilde{\mathcal{O}}(\sqrt{n}/\alpha)$ -approximate SIVP (or SVP) on tensor ideal lattices in $K_{(T)}$ to m -R-DLWE $_{q,\Upsilon_\alpha}$. Alternatively, for any $l \geq 1$, we can replace the target problem by the problem of solving m -R-DLWE $_{q,D_\xi}$ given only l samples, where $\xi = \alpha \cdot (nl/\log nl)^{1/4}$.*

³ $U(R_q^\vee)$ represents the uniform distribution over R_q^\vee

Discretizing the b component In practical applications [21], we usually deal with a version of the hardness problem where the error distribution is discrete. That is, instead of working with an error distribution ψ over $K_{(T),\mathbb{R}}$, we have to deal with an m -RLWE distribution $A_{s,\chi}$ where χ is a discrete error distribution over R^\vee therefore resulting in an element b that belongs to R_q^\vee .

Here, we present a variant of Definition 3 that we call m -R-DLWE $_{q,\chi}$ where we have a given number of samples from χ instead of ψ , and we have the problem of distinguishing between samples from $A_{s,\chi}$ and uniform samples from $R_q \times R_q^\vee$.

The procedure we have to follow in order to guarantee the hardness of the discrete version is basically the same as the procedure followed in [16]. Therefore, we include the main lemmas that explain the hardness of the discrete version together with some relevant explanations about the considerations needed for our multivariate case.

The following Lemma 2 states that if m -R-DLWE $_{q,\psi}$ is hard with l samples, then m -R-DLWE $_{q,\chi}$ is also hard for the same number of samples, with χ the distribution obtained from $\lfloor p \cdot \psi \rfloor_{w+pR^\vee}$ and p and q coprime integers.

Lemma 2 (Extended version of Lemma 2.23 in [16]). *Let p and q coprime integers, and $\lfloor \cdot \rfloor$ a valid discretization to cosets of pR^\vee . There exists an efficient transformation that on input $w \in R_p^\vee$ and a pair in $(a', b') \in R_q \times K_{(T),\mathbb{R}}/qR^\vee$ outputs $(a = pa' \bmod qR, b) \in R_q \times R_q^\vee$ with the following considerations: if the input pair is uniformly distributed then so is the output pair; and if the input pair is distributed according to the multivariate ring-LWE distribution $A_{s,\psi}$ for some unknown $s \in R^\vee$ and distribution ψ over $K_{(T),\mathbb{R}}$, then the output is distributed according to $A_{s,\chi}$ where we have that $\chi = \lfloor p \cdot \psi \rfloor_{w+pR^\vee}$.*

In practical applications [21] it is also common to have two additional changes with respect to the previous definition of the average-case decision version: a) instead of sampling a and s from R_q and R_q^\vee respectively, both are usually sampled from R_q . In general, we are in a different situation when we do this, however the works that consider that s belongs to R_q deal with a particular type of cyclotomic fields where m_i is a power of two. It can be shown that for this particular type of cyclotomic fields both definitions are equivalent, so it does not introduce additional drawbacks to the hardness reduction; b) instead of a uniform s , s is chosen from the error distribution (this is known as “normal form”) in practical cases, hence having a short secret key.

In order to show that the variant with short error (R-DLWE $_{q,\chi}$) is as hard as the original R-DLWE $_{q,\psi}$, the proof of Lyubashevsky *et al.* [16] follows the technique of [1]. Their results can be easily adapted to our more general case, so we include below the relevant lemma:

Lemma 3 (Extended version of Lemma 2.24 in [16]). *Let p and q be positive coprime integers, $\lfloor \cdot \rfloor$ be a valid discretization to cosets of pR^\vee , and w be an arbitrary element in R_p^\vee . If m -R-DLWE $_{q,\psi}$ is hard given some number l of samples, then so is the variant of m -R-DLWE $_{q,\chi}$ where the secret is sampled from $\chi = \lfloor p \cdot \psi \rfloor_{w+pR^\vee}$, given $l - 1$ samples.*

The proof of the previous lemma relies on how to use an oracle of the second problem to solve the first one. The difference with respect the proof presented in [16] lies on how to compute the fraction of invertible elements of R_q . In order to resolve this, we resort to the following claim about cyclotomic fields:

Claim 1 (Claim 2.25 in [16]). *Consider the m -th cyclotomic field of degree $n = \phi(m)$ for some $m \geq 2$. Then for any $q \geq 2$, the fraction of invertible elements in R_q is at least $1/\text{poly}(n, \log q)$.*

In our case, we work with the tensor of cyclotomic fields $K_{(T)} = \bigotimes_{i \in [l]} K_i$; for each cyclotomic field K_i , the fraction of irreducible elements in $\mathcal{O}_{K_i}/\langle q \rangle$ is at least $1/\text{poly}(\phi(m_i), \log q)$ with $q \geq 2$ and with $q \equiv 1 \pmod{m_i}$ for all $i \in [l]$. When working in the tensor of the different polynomial rings over \mathbb{Z}_q , if an element is invertible, the corresponding elements belonging to each \mathcal{O}_{K_i} must be invertible too (same explanation as in Kronecker product of matrices, Section 2.1). Then, the fraction of invertible elements in $R_q = \bigotimes_{i \in [l]} \mathcal{O}_{K_i}/\langle q \rangle$ is at least the product of the fractions of each ring of integers $1/\text{poly}(\prod_{i \in [l]} \phi(m_i), \log q) = 1/\text{poly}(n, \log q)$, and Lemma 3 follows.

4 Proof sketch of the hardness of the multivariate Ring Learning with Errors problem

This section introduces the main theorems together with their proofs for the different reductions of the m -RLWE problem. The proof can be divided in two main parts, described in the following paragraphs.

Hardness Search-LWE The first part achieves a quantum reduction from approximate SVP on ideal lattices over R to the search version of m -RLWE. The goal of the search version is to recover the secret key s . The procedure follows the techniques considered by Lyubashevsky *et al.* [14] and Regev [24].

The main contribution here is to extend their tools to the more general case of the tensor of cyclotomic fields (or even the tensor of more general fields). For this purpose, we use the interactive quantum reduction for general lattices of Regev together with the corresponding tools that we can find on algebraic number theory; i.e., the Chinese Remainder Theorem and the canonical embedding that were used by Lyubashevsky *et al.* but adapted to our multivariate case.

Pseudorandomness of m -RLWE The main purpose of this part is to show that the m -RLWE distribution is pseudorandom, that is, there exists a reduction from the search problem, discussed in the first part, to the decision variant of the hardness problem. We present two different versions of the hardness problem: one for the decision problem with a nonspherical distribution in the canonical embedding, and another one for the decision problem with a spherical distribution but with a bounded number of samples. Additionally, when assuming the hardness of the search problem with a fixed spherical Gaussian error distribution, we also have hardness of the decision version with the same error distribution.

Again, the main contribution of our work relies on proving that the multivariate samples following the m -RLWE distribution are pseudorandom, therefore generalizing the results of [14] to the case of multivariate elements. The main needed properties are those related to the decomposition of $\langle q \rangle$ into n prime ideals and the use of the automorphisms that allow us to permute the prime ideals.

4.1 Hardness Search-LWE

For this section, let $K_{(T)} = \bigotimes_{i \in [l]} K_i$ of degree n denote the tensor of l arbitrary number fields and $R = \bigotimes_{i \in [l]} \mathcal{O}_{K_i}$ the corresponding tensor of rings of integers. The results can be applied to an arbitrary number field, so in this section we do not have to consider the specific case of cyclotomic fields.

Theorem 2 (Extended Theorem 4.1 of Lyubashevsky *et al.* [14]). *Let $K_{(T)}$ be a tensor of arbitrary number fields with degree n_i each and R the tensor of the corresponding ring of integers. Let $\alpha = \alpha(n) > 0$, and let $q = q(n) \geq 2$ be such that $\alpha q \geq 2 \cdot \omega(\sqrt{\log n})$, where $\omega(f(n))$ denotes a function that asymptotically grows faster than $f(n)$. For some negligible $\epsilon = \epsilon(n)$, there is a probabilistic polynomial-time quantum reduction from $K_{(T)}$ -DGS $_\gamma$ to m -R-LWE $_{q, \Psi_{\leq \alpha}}$, where*

$$\gamma = \max \{ \eta_\epsilon(\mathcal{I}) \cdot (\sqrt{2}/\alpha) \cdot \omega(\sqrt{\log n}), \sqrt{2n}/\lambda_1(\mathcal{I}^\vee) \}$$

Here $K_{(T)}$ -DGS $_\gamma$ denotes the discrete Gaussian sampling problem [24, 14] where given an ideal \mathcal{I} in $K_{(T)}$ and a number $s \geq \gamma = \gamma(\mathcal{I})$, we have to generate samples from $D_{\mathcal{I}, s}$. The proof of this theorem is shown in Appendix B.

Regev [24] showed that we have easy reductions from standard lattice problems to DGS. As Lyubashevsky *et al.* [14] assert, combining lemmas 4 and 6 we have $\eta_\epsilon(\mathcal{I}) \leq \lambda_n(\mathcal{I}) \cdot \omega(\sqrt{\log n})$ (see Appendix A.2 for the definition of the smoothing parameter η_ϵ) for any fractional ideal \mathcal{I} and negligible $\epsilon(n)$, and we also have that samples from $D_{\mathcal{I}, \gamma}$ have length at most $\gamma\sqrt{n}$ with overwhelming probability. This is also valid in our case.

Analogously, an oracle for $K_{(T)}$ -DGS $_\gamma$ with $\gamma = \eta_\epsilon(\mathcal{I}) \cdot \tilde{O}(1/\alpha)$ implies an oracle for $\tilde{O}(\sqrt{n}/\alpha)$ -approximate SIVP on ideal lattices in the tensor field $K_{(T)}$.

When each K_i is a cyclotomic field, we also have $\lambda_n(\mathcal{I}) = \lambda_1(\mathcal{I})$ for any fractional ideal \mathcal{I} , as for each shortest nonzero $v \in \mathcal{I}$, if we multiply it by different combinations of $\zeta_{m_1}^{e_1-1} \otimes \dots \otimes \zeta_{m_l}^{e_l-1}$ with $e_i \in [\phi(m_i)]$, it yields a total of n independent elements of equal length, that is, we have an oracle for $\tilde{O}(\sqrt{n}/\alpha)$ -approximate SVP.

It is important to note that as the error distribution is added modulo R^\vee in the definition of m -RLWE, the condition $\alpha < \eta_\epsilon(R^\vee)$ must be satisfied for all negligible $\epsilon(n)$ for the problem to be solvable.

4.2 Pseudorandomness of m -RLWE

In this section, we particularize again $K_{(T)} = \bigotimes_{i \in [l]} K_i$ and $R = \bigotimes_{i \in [l]} \mathcal{O}_{K_i}$ for the cyclotomic case $K_i = \mathbb{Q}(\zeta_{m_i})$ with ζ_{m_i} a primitive m_i -th root of unity. We also consider the prime $q \equiv 1 \pmod{m_i}$ for all $i \in [l]$ and we have that it is $\text{poly}(n)$ -bounded, where $n = \prod_{i \in [l]} \phi(m_i)$ is the degree of the considered multivariate polynomials.

We recall that $K_{(T)}$ has a set of n different automorphisms τ_j with $j \in [n]$ (see Equation (3)) and when working over q , we have that $\langle q \rangle = \prod_{i \in [l]} \mathfrak{q}_i$ splits into a product of prime ideals \mathfrak{q}_i where the automorphisms satisfy $\bigotimes_{i \in [l]} \tau_{k_i}^{(i)}(\mathfrak{q}_j) = \mathfrak{q}_{j'}$ with $k_i \in \mathbb{Z}_{m_i}^*$ and $j, j' \in [n]$ (for more details we refer the reader to Appendix A).

In the following we present the main theorems about the different reductions from the search version of m -RLWE (see Definition 2 and Theorem 2 about the reduction over worst-case lattice problems) to the average-case decision problem m -R-DLWE (see Definition 3).

Theorem 3 (Extended Theorem 5.1 of Lyubashevsky *et al.* [14]). *Let R and q be as shown previously and let $\alpha q \geq \eta_\epsilon(R^\vee)$ for some negligible $\epsilon = \epsilon(n)$. Then, there is a randomized polynomial-time reduction from m -R-LWE $_{q, \Psi_{\leq \alpha}}$ to m -R-DLWE $_{q, \Upsilon_\alpha}$.*

In order to prove the previous theorem we need four more reductions that are described

in the following discussion.

$$\begin{aligned} \text{LWE}_{q,\Psi} &\xrightarrow[\text{Lemma 16}]{\text{Automorphisms}} \mathfrak{q}_i\text{-LWE}_{q,\Psi} \xrightarrow[\text{Lemma 18}]{\text{Search/Decision}} \text{WDLWE}_{q,\Psi}^i \\ &\quad \text{WDLWE}_{q,\Psi}^i \xrightarrow[\text{Lemma 19}]{\text{Worst/Average}} \text{DLWE}_{q,\Upsilon}^i \xrightarrow[\text{Lemma 20}]{\text{Hybrid}} \text{DLWE}_{q,\Upsilon} \end{aligned}$$

The details of the proof follow the steps of Lyubashevsky *et al.* [14], which, conversely, follows similar steps to the reductions of [24], the main point being the use of the automorphisms to recover the secret key s when only knowing the secret key relative to one prime ideal \mathfrak{q}_i (Lemma 16).

An additional needed step is the randomization of the error distribution (sampled from Υ) such that the error is invariant under the different field automorphisms (see Lemma 19) because the different $\psi \in \Psi_{\leq \alpha}$ are not necessarily invariant under the field automorphisms. Equivalently, if this reduction randomizing the error distribution is not desirable, we can apply a bound on the number of samples for considering a result about pseudorandomness of m -RLWE with a fixed spherical noise distribution.

Theorem 4 (Extended Theorem 5.2 of Lyubashevsky *et al.* [14]). *Let R , q and α be as in Theorem 3 and let $l \geq 1$. There is a randomized polynomial-time reduction from solving m -R-LWE $_{q,\Psi_{\leq \alpha}}$ to solving m -R-DLWE $_{q,D_\xi}$ given only l samples, where $\xi = \alpha \cdot (nl / \log(nl))^{1/4}$.*

In this case, we have a similar reduction to the one in Theorem 3 but considering a different lemma (Lemma 22 instead of Lemma 19 in one of the steps).

$$\text{WDLWE}_{q,\Psi}^i \xrightarrow[\text{Lemma 22}]{\text{Worst/Average}} \text{DLWE}_{q,D_\xi}^i \xrightarrow[\text{Lemma 20}]{\text{Hybrid}} \text{DLWE}_{q,D_\xi}$$

It is interesting to note that if we assume hardness of the search version with a spherical error distribution LWE $_{q,D_\xi}$, then we also have a reduction for the pseudorandomness with a spherical error, but simplifying Lemma 19 instead of resorting to sampling from the Υ distribution.

Theorem 5 (Extended Theorem 5.3 of Lyubashevsky *et al.* [14]). *Let R , q and α be as in Theorem 3. There exists a randomized polynomial-time reduction from solving m -R-LWE $_{q,D_\alpha}$ to solving m -R-DLWE $_{q,D_\alpha}$.*

The detailed proofs for these three theorems along with the lemmas involved in the security reductions for m -RLWE are included in Appendix C.

5 Conclusions

In this work we have presented a multivariate version of the well-known Ring Learning with Errors (RLWE) problem to a multivariate version working over the tensor product of number fields, denoted m -RLWE, which finds application in secure signal processing scenarios. We have adapted and generalized the techniques of Lyubashevsky *et al.* [14] to the tensor product of number fields and achieved a reduction of the m -RLWE problem to hardness problems over ideal lattices, hence proving its security.

A Fundamental Concepts of Lattices and Algebraic Number Theory

This appendix presents the fundamental concepts of lattices and algebraic number theory and extends them to the more general case of a tensor number field on which m -RLWE is mainly based.

A.1 The Space $H_{(T)} = \bigotimes_i H_i$

When working with cyclotomic fields, it is useful to work with the subspace $H \subseteq \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$ with $s_1 + 2s_2 = n$, where the tuple (s_1, s_2) is called the signature of the number field, and H satisfies:

$$H = \{(x_1, \dots, x_n) \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} \text{ such that } x_{s_1+s_2+j} = \bar{x}_{s_1+j}, \forall j \in [s_2]\} \subseteq \mathbb{C}^n \quad (1)$$

An orthonormal basis $\{\mathbf{h}_j\}_{j \in [n]}$ for H can be defined as:

$$\mathbf{h}_j = \begin{cases} \mathbf{e}_j & \text{if } j \in [s_1] \\ \frac{1}{\sqrt{2}}(\mathbf{e}_j + \mathbf{e}_{j+s_2}) & \text{if } s_1 < j \leq s_1 + s_2 \\ \frac{\sqrt{-1}}{\sqrt{2}}(\mathbf{e}_{j-s_2} - \mathbf{e}_j) & \text{if } s_1 + s_2 < j \leq s_1 + 2s_2 \end{cases} \quad (2)$$

where the vectors \mathbf{e}_j are the vectors of the standard basis in \mathbb{R}^n .

Finally, each element $a = \sum_{j \in [n]} a_j \mathbf{h}_j \in H$ (where all $a_j \in \mathbb{R}$) has its own l_p norm defined as above.

For our purposes, we define the subspace $H_{(T)} = \bigotimes_{i \in [l]} H_i$ as the tensor product of l subspaces H_i , each equivalent to the subspaces previously introduced.

In particular, if we see each element belonging to each H_i as a different linear transformation, we are actually working with the Kronecker product of the different subspaces H_i . Hence, the new basis will be the result of the Kronecker product of the original basis of each H_i , therefore having an orthonormal basis for $H_{(T)}$ given by $\{\mathbf{h}_j\}_{j \in [n]}$, where we can define the following mapping for j

$$j = 1 + \sum_{i \in [l]} (j_i - 1) \prod_{d \in [i]} n_{d-1}, \quad (3)$$

being $\mathbf{h}_j = \bigotimes_{i \in [l]} \mathbf{h}_{j_i}^{(i)}$ the new form of the basis vectors, and where $n = \prod_{i \in [l]} n_i$ and each $\{\mathbf{h}_{j_i}^{(i)}\}_{j_i \in [n_i]}$ is the corresponding orthonormal basis of each $H_i \subseteq \mathbb{C}^{n_i}$ for $i \in [l]$ and $n_0 = 1$. This expression is used when indexing the embeddings (see Appendix A.3.2) and automorphisms (see Section 2) that can be performed in a tensor field.

A.2 Lattice background

A lattice in our multivariate setting is defined as an additive subgroup of $H_{(T)} = \bigotimes_{i \in [l]} H_i$. We only work with lattices of full rank, which are obtained as the set of all integer linear combinations of a set of n linear independent basis vectors $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\} \subset H_{(T)}$.⁴

$$\Lambda = \mathcal{L}(\mathbf{B}) = \left\{ \sum_{i \in [n]} z_i \mathbf{b}_i \text{ such that } \mathbf{z} \in \mathbb{Z}^n \right\} \quad (4)$$

⁴As we work with the Kronecker product of a basis for each subspace H_i , we can exploit the properties of the Kronecker product to work with bases for each H_i satisfying the corresponding properties.

The minimum distance $\lambda_1(\Lambda)$ of a lattice Λ for the norm $\|\cdot\|$ is given with the length of the shortest nonzero lattice vector, that is, $\lambda_1(\Lambda) = \min_{\mathbf{x} \in \Lambda/\mathbf{x} \neq \mathbf{0}} \|\mathbf{x}\|$.

The dual lattice of $\Lambda \subset H_{(T)}$ is defined as $\Lambda^* = \{\mathbf{x} \in H_{(T)} \text{ such that } \langle \Lambda, \mathbf{x} \rangle \subseteq \mathbb{Z}\}$ and it satisfies $(\Lambda^*)^* = \Lambda$.

Gaussian Measures The results explained in [14] for nonspherical Gaussian distributions can be easily extended to our case. So we repeat here some of the concepts presented for Gaussian measures but adapted to our tensor setting.

We consider the Gaussian function $\rho_r : H \rightarrow (0, 1]$ with $r > 0$ as

$$\rho_r(\mathbf{x}) = \exp(-\pi \|\mathbf{x}\|^2 / r^2).$$

A continuous Gaussian probability distribution can be obtained by normalizing the previous function in such a way that we have D_r with a density function $r^{-n} \rho_r(\mathbf{x})$. When we extend this to the non spherical Gaussian case, we consider the vector $\mathbf{r} = \bigotimes_{i \in [l]} \mathbf{r}_i$ where each $\mathbf{r}_i = (r_{i,1}, \dots, r_{i,n_i}) \in (\mathbb{R}^+)^{n_i}$ and whose components satisfy $r_{i,j+s_1+s_2} = r_{i,j+s_1}$. Finally, a sample from $D_{\mathbf{r}}$ is given by $\sum_{i \in [n]} x_i \mathbf{h}_i$ where $x_j = \prod_{i \in [l]} x_{j_i}^{(i)}$ where each x_j is drawn independently from the Gaussian distribution D_{r_j} over \mathbb{R} being r_j equal to $\prod_{i \in [l]} r_{i,j_i}$ and using the mapping between $\{j\}_{j \in [n]}$ and $\{j_i\}_{j_i \in [n_i], i \in [l]}$ given by equation (3).

Next, we include several results about the Gaussian distributions that are needed for this work.

Definition 6 (Smoothing parameter). *The smoothing parameter $\eta_\epsilon(\Lambda)$ for a lattice Λ and real $\epsilon > 0$ is defined as the smallest r such that $\rho_{1/r}(\Lambda^* \setminus \{\mathbf{0}\}) \leq \epsilon$.*

In addition, several important lemmas from [14], [19], [24] and [2] about the relation between the smoothing parameter and properties of lattices are included below.

Lemma 4 (Lyubashevsky *et al.* [14] Lemma 2.2, Micciancio and Regev [19] Lemmas 3.2 and 3.3). *For any n -dimensional lattice Λ , we have $\eta_{2^{-2n}}(\Lambda) \leq \sqrt{n}/\lambda_1(\Lambda^*)$ and $\eta_\epsilon(\Lambda) \leq \sqrt{\ln(n/\epsilon)} \lambda_n(\Lambda)$ for all $0 < \epsilon < 1$.*

Lemma 5 (Lyubashevsky *et al.* [14] Lemma 2.3, Micciancio and Regev [19] Lemma 4.1, Regev [24] Claim 3.8). *For any lattice Λ , $\epsilon > 0$, $r \geq \eta_\epsilon(\Lambda)$, and $\mathbf{c} \in H_{(T)}$, the statistical distance⁵ between $(D_r + \mathbf{c}) \bmod \Lambda$ and the uniform distribution modulo Λ is at most $\epsilon/2$. Alternatively, we have $\rho_r(\Lambda + \mathbf{c}) \in \left[\frac{1-\epsilon}{1+\epsilon}, 1\right] \rho_r(\Lambda)$.*

Let a lattice Λ , a point $\mathbf{u} \in H_{(T)}$ and $r > 0$ with $r \in \mathbb{R}$, the discrete Gaussian probability distribution over $\Lambda + \mathbf{u}$ with parameter r can be defined as $D_{\Lambda+\mathbf{u},r}(\mathbf{x}) = \frac{\rho_r(\mathbf{x})}{\rho_r(\Lambda+\mathbf{u})}$ for all $\mathbf{x} \in \Lambda + \mathbf{u}$.

Lemma 6 (Banaszczyk [2], Lemma 1.5 (i)). *For any n -dimensional lattice Λ and $r > 0$, a sample point from $D_{\Lambda,r}$ has Euclidean norm at most $r\sqrt{n}$, except with probability at most 2^{-2n} .*

Lemma 7 (Regev [24]). *Let Λ be a lattice, let $\mathbf{u} \in H$ be any vector, and let $r, s > 0$ be reals. Assume that $1/\sqrt{1/r^2 + 1/s^2} \geq \eta_\epsilon(\Lambda)$ for some $\epsilon < 1/2$. Consider the continuous distribution Y on H obtained by sampling from $D_{\Lambda+\mathbf{u},r}$ and then adding an element drawn independently from D_s . Then, the statistical distance between Y and $D_{\sqrt{r^2+s^2}}$ is at most 4ϵ .*

⁵The statistical distance $\Delta(X, Y)$ between two continuous random variables X and Y over \mathbb{R}^n with probability density functions T_1 and T_2 is defined as $\Delta(X, Y) = \frac{1}{2} \int_{\mathbb{R}^n} |T_1(r) - T_2(r)| dr$. For more details we refer the reader to [19] and [24].

A.3 Algebraic Number Theory background

This appendix covers the main concepts related to number fields that are used in the papers [14] and [16]; we highlight the theorems and lemmas that are fundamental to our proof, so even when they have already been presented in the literature, we include them here for completeness and to make our work self-contained. We also particularize some of the results to the case of cyclotomic fields; for further details, we refer the reader to the previous cited papers or to any introductory book on the subject [12].

The concepts about algebraic number theory presented here are necessary to show which are the main changes needed to extend the proof of Lyubashevsky *et al.* to the generic multidimensional case (not only coprime factors), as explained in Section 4.

A.3.1 Number fields

A number field is defined as a field extension $K = \mathbb{Q}(\varsigma)$ where the element ς is incorporated to the field of rationals. This element ς satisfies $f(\varsigma) = 0$ for an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ denoted minimal polynomial of ς . The degree n of a number field is the degree of its minimal polynomial.

We can also see the number field K as an n -dimensional vector space over \mathbb{Q} where $\{1, \varsigma, \dots, \varsigma^{n-1}\}$ is called the power basis of the field K . Of course, we have an isomorphism between K and $\mathbb{Q}[x]/f(x)$.

In this work, we have a special interest on cyclotomic fields, which are those fields where $\varsigma = \varsigma_m$, for some natural number m , is an m -th primitive root of unity and the minimal polynomial of ς_m is the m -th cyclotomic polynomial $\Phi_m(x) = \prod_{i \in \mathbb{Z}_m^*} (x - \omega_m^i) \in \mathbb{Z}[x]$, where $\omega_m \in \mathbb{C}$ is any primitive m -th complex root of unity (for example $\omega_m = e^{2\pi\sqrt{-1}/m}$). It is important to note that the different powers ω_m^i of $\Phi_m(x)$ are the m -th roots of unity in \mathbb{C} and that the degree of $\Phi_m(x)$ is $n = \phi(m)$, where $\phi(m)$ is the Euler's totient function.

In general, there is no bound on the number of elements that can be added, so we could have $K = \mathbb{Q}(\varsigma_{m_1}, \dots, \varsigma_{m_l})$, that is isomorphic to the cyclotomic field $\mathbb{Q}(\varsigma_m) = \bigotimes_{i \in [l]} \mathbb{Q}(\varsigma_{m_i})$ when $m = \prod_{i \in [l]} m_i$ has a prime-power decomposition and each ς_{m_i} is a m_i -th primitive root of unity (See [16]).

Therefore, we can see our scheme as a generalization of the previous tensor product of cyclotomic fields, where we can have a non prime tensor decomposition of m (the same power cyclotomic can appear several times in the expression).

A.3.2 Embeddings and Geometry

Here, we describe the embeddings that can be defined in a general number field together with the canonical geometry that we can consider thanks to these embeddings.

A number field $K = \mathbb{Q}(\varsigma)$ of degree n has exactly n embeddings $\sigma_i : K \rightarrow \mathbb{C}$ where each of these embeddings maps ς to a different complex root of its minimal polynomial f . The number of real embeddings is denoted s_1 and the number of pairs of complex embeddings is denoted by s_2 (each complex root has a conjugate), so we have $n = s_1 + 2s_2$ (the pair (s_1, s_2) is called the signature of the number field).

The canonical embedding is defined as

$$\sigma : K \rightarrow \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2},$$

where $\sigma(x) = (\sigma_1(x), \dots, \sigma_n(x))^T$. We let $\{\sigma_i\}$ with $i = 1, \dots, s_1$ be the real embeddings and $\sigma_{s_1+s_2+j} = \bar{\sigma}_{s_1+j}$ with $j = 0, \dots, s_2 - 1$ be the complex embeddings.

For our purposes it is useful to redefine the embedding of $\bigotimes_{i \in [l]} K_i$ as in [16] with the corresponding reordering of the $\sigma_i(x)$. Therefore, we have $\sigma(\bigotimes_{i \in [l]} a_i) = \bigotimes_{i \in [l]} \sigma^{(i)}(a_i)$ and instead of considering the signature (s_1, s_2) , each $\sigma^{(i)}$ is defined as $\sigma^{(i)} : K_i \rightarrow \mathbb{C}^{\mathbb{Z}_{m_i}^*}$ (for the particular case of cyclotomic fields with $m_i > 2$ there are no real roots, so we have $s_1 = 0$).

Now, we have a bijective map $g^{(i)} : [\phi(m_i)] \rightarrow \mathbb{Z}_{m_i}^*$ that allows us to represent each embedding with a new set of indices as $\sigma^{(i)}(x) = \left(\sigma_{g^{(i)}(1)}^{(i)}(x), \dots, \sigma_{g^{(i)}(\phi(m_i))}^{(i)}(x) \right)^T$ in such a way that if $j_i \in \mathbb{Z}_{m_i}^* = g^{(i)}([\phi(m_i)])$, the relation between the complex conjugates is $\sigma_{j_i}^{(i)} = \bar{\sigma}_{m_i - j_i}^{(i)}$. Finally, the tensoring of the different embeddings $\bigotimes_{i \in [l]} \sigma^{(i)}(a_i)$ reduces over $H_{(T)}$ in a Kronecker product of the images obtained in each different subspace H_i .

By virtue of this canonical embedding, there exists a ring homomorphism from $\bigotimes_{i \in [l]} K_i$ to $\bigotimes_{i \in [l]} H_i$ where each $H_i \subset \mathbb{C}^{\mathbb{Z}_{m_i}^*}$, and where multiplication and addition are element-wise. Thanks to this, we can define geometric norms over $\bigotimes_{i \in [l]} K_i$ considering the presented tensor subspace $H_{(T)}$. Therefore, for any $x \in K_{(T)}$ and any $p \in [1, \infty]$, we consider $\|x\|_p = \|\sigma(x)\|_p = \left(\sum_{j \in [n]} |\sigma_j(x)|^p \right)^{1/p}$ with $p < \infty$ and $\max_{j \in [n]} |\sigma_j(x)|$ for $p = \infty$, where each $\sigma_j(x) = \prod_{i \in [l]} \sigma_{g^{(i)}(j_i)}^{(i)}(x)$ following the mapping indicated in Equation (3), and $j_i \in [\phi(m_i)]$, $j \in [n]$ such that $n = \prod_{i \in [l]} \phi(m_i)$ with $\phi(m_i) = n_i$.

Analogously, the canonical embedding allows us to work with the Gaussian distribution $D_{\mathbf{r}}$ with $\mathbf{r} \in (\mathbb{R}^+)^n$ over $\bigotimes_i H_i$ as a distribution over $\bigotimes_i K_i$. Actually, the distribution $D_{\mathbf{r}}$ is over $K_{(T), \mathbb{R}} = K_{(T)} \otimes_{\mathbb{Q}} \mathbb{R}$ which is also isomorphic to $H_{(T)}$ as a real vector space.⁶ However, it is more helpful to ignore the distinction between $K_{(T)}$ and $K_{(T), \mathbb{R}}$ and to approximate the latter by the former using enough precision (in order to represent real numbers with rational numbers).

A.3.3 Trace and Norm

Here we present the basic concepts of trace and norm over number fields that were proposed in previous works. Section 2 highlights which are the changes needed and how we can work with them when we have the tensor product of non coprime cyclotomic fields.

The trace $\text{Tr} = \text{Tr}_{K/\mathbb{Q}} : K \rightarrow \mathbb{Q}$ and norm $N = N_{K/\mathbb{Q}} : K \rightarrow \mathbb{Q}$ are defined as:

$$\text{Tr}(x) = \sum_{i \in [n]} \sigma_i(x), \quad N(x) = \prod_{i \in [n]} \sigma_i(x). \quad (5)$$

In addition, the trace is a linear function in \mathbb{Q} because $\text{Tr}(a + b) = \text{Tr}(a) + \text{Tr}(b)$ and $\text{Tr}(ca) = c\text{Tr}(a)$ for all $a, b \in K$ and $c \in \mathbb{Q}$. It is also important to note that $\text{Tr}(a \cdot b) = \sum_i \sigma_i(a) \sigma_i(b)$.

Even though we will do more emphasis later, we note that when working with tensor products $K_{(T)} = \bigotimes_i K_i$, resorting to the fact that $\sigma(\bigotimes_i a_i) = \bigotimes_i \sigma^{(i)}(a_i)$ the corresponding trace satisfies $\text{Tr}_{K_{(T)}/\mathbb{Q}}(\bigotimes_i a_i) = \prod_i \text{Tr}_{K_i/\mathbb{Q}}(a_i)$.

A.3.4 Tensor Ring of Integers and its Ideals

This appendix revises some basic properties of the ring of integers of a number field and its ideals. Although we are considering cyclotomic number fields $K_i = \mathbb{Q}(\zeta_{m_i})$, these

⁶We will use $K_{(T)}$ instead of $K_{(T), \mathbb{R}}$ unless the distinction is relevant.

results apply to more general number fields. The ring of integers of a number field is denoted \mathcal{O}_{K_i} and it is defined as the set of elements belonging to K_i that satisfy a monic polynomial $f(x)$ with coefficients belonging to the integers, that is, elements $a \in K_i$ such that $f(a) = 0$.

It can be seen that \mathcal{O}_{K_i} is a free \mathbb{Z} -module with rank the degree of K_i (when working with cyclotomic fields this degree is $\phi(m_i)$), and that its \mathbb{Z} -basis $B_i = \{b_1^{(i)}, \dots, b_n^{(i)}\} \subset \mathcal{O}_{K_i}$ results to be a \mathbb{Q} -basis for K_i and also a \mathbb{R} -basis for $K_i \otimes \mathbb{R}$.

We work with the result of the tensor product of the different rings of integers which corresponds to each number field, that is, for the tensor number field $K_{(T)} = \bigotimes_{i \in [l]} K_i$ we consider the tensor ring of integers $R = \bigotimes_{i \in [l]} \mathcal{O}_{K_i}$. All the properties introduced for the ring of integers in [14] are also valid when working with ideals of the new multivariate polynomial ring R .

Firstly, we could see R as a \mathbb{Z} -module with rank $n = \prod_{i \in [l]} \phi(m_i)$ and its \mathbb{Z} -basis would be $\bigotimes_{i \in [l]} B_i \subset R$ that also results to be a \mathbb{Q} -basis for $K_{(T)}$ and a \mathbb{R} -basis for $K_{(T), \mathbb{R}}$.

Next, we include some important facts about the ideals of R . An integral ideal (a.k.a. ideal) of R is an additive subgroup that is closed under multiplication by R , that is, $r \cdot x \in \mathcal{I}$ for any $r \in R$ and $x \in \mathcal{I}$. In order to generate an ideal \mathcal{I} of R , it can be shown that there exist two different elements $g_1, g_2 \in \mathcal{O}_K$ whose R -linear combinations generate $\mathcal{I} = \langle g_1, g_2 \rangle$. An ideal is also a free \mathbb{Z} -module of rank n , so we have some basis $\{u_1, \dots, u_n\} \subset R$.

The norm of an ideal is its corresponding index as an additive subgroup, that is, $N(\mathcal{I}) = |R : \mathcal{I}|$. The sum $\mathcal{I} + \mathcal{J}$ is also an ideal whose elements are all the pairs $x + y$ with $x \in \mathcal{I}$ and $y \in \mathcal{J}$, the product ideal $\mathcal{I}\mathcal{J}$ is the set of all finite sums of pairs xy with $x \in \mathcal{I}$ and $y \in \mathcal{J}$. The norm of ideals generalizes the previous definition of norm in the following way $N(\langle x \rangle) = |N(x)|$ with $x \in R$ and $N(\mathcal{I}\mathcal{J}) = N(\mathcal{I})N(\mathcal{J})$.

We say that two ideals \mathcal{I} and \mathcal{J} are coprime (or relatively prime) if $\mathcal{I} + \mathcal{J} = R$. An ideal $\mathfrak{p} \subsetneq R$ is prime if whenever $ab \in \mathfrak{p}$ for some $a, b \in R$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. An ideal \mathfrak{p} of R is prime if and only if it is maximal. The ring R has unique factorization on ideals, that is, every ideal of R can be expressed as a unique product of powers of prime ideals.

A fractional ideal $\mathcal{I} \subset K$ satisfies $d\mathcal{I} \subseteq R$ where $d\mathcal{I}$ is an integral ideal for some $d \in R$. Its norm is defined as $N(\mathcal{I}) = N(d\mathcal{I})/|N(d)|$.

A.3.5 Ideal Lattices

This work relies on the lattices embedded by the fractional ideals in $K_{(T)}$ under the canonical embedding. Next, we describe some of their properties. A fractional ideal \mathcal{I} has a \mathbb{Z} -basis $U = \{u_1, \dots, u_n\}$. Then, under the canonical embedding σ , the ideal yields a rank- n ideal lattice $\sigma(\mathcal{I})$ with basis $\{\sigma(u_1), \dots, \sigma(u_n)\} \subset H_{(T)}$. The lattice embedded by an ideal is commonly identified by the ideal, so we consider the minimum distance $\lambda_1(\mathcal{I})$ of an ideal.

The absolute discriminant Δ_K is defined for a field K . We generalize this term to the tensor field $K_{(T)}$, considering $\Delta_{K_{(T)}}$ as the square of the fundamental volume of the embedded lattice $\sigma(R)$. We also have $\Delta_{K_{(T)}} = |\det(\text{Tr}(b_i \cdot b_j))|$, where $\{b_1, \dots, b_n\}$ is an integral basis of R . Therefore, we can define the fundamental volume of an ideal lattice $\sigma(\mathcal{I})$ as $N(\mathcal{I}) \cdot \sqrt{\Delta_{K_{(T)}}}$.

Now we include an important lemma that gives upper and lower bounds on the minimum distance of an ideal lattice.

Lemma 8 (Extended version of Lyubashevsky *et al.* [14] Lemma 2.9, Peikert and Rosen [23] detailed proof). *For any fractional ideal \mathcal{I} in a tensor field $K_{(T)}$ of degree n , and in*

any l_p -norm for $p \in [1, \infty]$,

$$n^{1/p} \cdot N(\mathcal{I})^{1/n} \stackrel{(a)}{\leq} \lambda_1(\mathcal{I}) \stackrel{(b)}{\leq} n^{1/p} \cdot N(\mathcal{I})^{1/n} \cdot \sqrt{\Delta_{K(T)}^{1/n}}. \quad (6)$$

The proof of the previous Lemma 8 follows analogously to the proofs of the Lemmas 6.1 (upper bound) and 6.2 (lower bound) in [23].

First, we start with the upper bound (b) following the guidelines of [23]. Considering $\|x\|_p \leq n^{1/p} \|x\|_\infty$ for $x \in K(T)$, we only need to prove the bound for the $p = \infty$ norm. For this purpose, we resort to Minkowski's Theorem 6 to bound the distance of λ_1^∞ :

Theorem 6 (Minkowski's Theorem). *Let Λ be any lattice of rank n and $\mathcal{B} \subseteq \text{span}(\Lambda)$ be any convex body symmetric about the origin having n -dimensional volume $\text{vol}(\mathcal{B}) > 2^n \cdot \det(\Lambda)$. Then \mathcal{B} contains some nonzero $x \in \Lambda$.*

Now, we consider the n -dimensional closed $\mathcal{C} = \{x \in H(T) : \|x\|_\infty \leq 1\}$, and each $\phi(m_i)$ -dimensional closed $\mathcal{C}^{(i)} = \{x \in H_i : \|x\|_\infty \leq 1\}$. Knowing that $H_i \subseteq \mathbb{R}^{s_1^{(i)}} \times \mathbb{C}^{2s_2^{(i)}}$, it can be shown that the volume of $\mathcal{C}^{(i)}$ is $2^{\phi(m_i)} \cdot (\pi/2)^{s_2^{(i)}}$, where $\phi(m_i) = s_1^{(i)} + s_2^{(i)}$ and finally being $2^n \cdot (\pi/2)^{\prod_{i \in [l]} s_2^{(i)}}$ the volume of \mathcal{C} .

Proceeding as in [23], we have for any $\beta > N^{1/n}(\mathcal{I}) \cdot \sqrt{\Delta_{K(T)}^{1/n}} \cdot (2/\pi)^{\prod_{i \in [l]} s_2^{(i)}/n}$

$$\text{vol}(\beta\mathcal{C}) = \beta^n \text{vol}(\mathcal{C}) > 2^n \cdot N(\mathcal{I}) \cdot \sqrt{\Delta_{K(T)}} = 2^n \cdot \det(\sigma(\mathcal{I})),$$

where by Minkowski's Theorem 6, we know that $\beta\mathcal{C}$ contains a nonzero point of $\sigma(\mathcal{I})$, therefore $\lambda_1^\infty \leq \beta$; consequently, it also satisfies the upper bound (b) of Lemma 8.

Regarding the lower bound (a), we follow the steps of the proof for Lemma 6.2 in [23]. For $1 \leq p \leq \infty$, by the arithmetic mean/geometric mean inequality we have:

$$\|x\|_p^p = \sum_{i \in [n]} |\sigma_i(x)|^p \geq n \cdot \left(\prod_{i \in [n]} |\sigma_i(x)|^p \right)^{1/n} = n \cdot |N(x)|^{p/n},$$

where by applying the p -root in both sides, it yields the considered lower bound (a) by considering that $|N(x)| \geq N(\mathcal{I})$ for any nonzero $x \in \mathcal{I}$ (for more details of both proofs we refer the reader to [23]). Here, it is important to note that resorting to the concepts presented in Appendix A.3.2, we can deal with the different embeddings, even when we are working with the tensor of number fields.

A.3.6 Duality

For any lattice \mathcal{L} in $K(T)$ (this is the \mathbb{Z} -span of any \mathbb{Q} -basis of $K(T)$), its dual is defined as:

$$\mathcal{L}^\vee = \{x \in K(T) : \text{Tr}(x\mathcal{L}) \subseteq \mathbb{Z}\}. \quad (7)$$

As in the “traditional” (non-tensor) number field case, using the canonical embedding, \mathcal{L}^\vee embeds as the complex conjugate of the dual lattice, that is, $\sigma(\mathcal{L}^\vee) = \bar{\sigma}_\mathcal{L}^*$. Taking this into account and considering also that $\mathcal{L} = \bigotimes_{i \in [l]} \mathcal{L}_i$ and the dual operation commutes the tensoring, we have:

$$\begin{aligned} \sigma(\mathcal{L}^\vee) &= \sigma(\bigotimes_i \mathcal{L}_i^\vee) = \bigotimes_i \sigma(\mathcal{L}_i^\vee) = \bigotimes_i \bar{\sigma}^*(\mathcal{L}_i) \\ &= \overline{\bigotimes_i \sigma^*(\mathcal{L}_i)} = \overline{(\bigotimes_i \sigma(\mathcal{L}_i))^*} = \overline{\sigma^*(\bigotimes_i \mathcal{L}_i)} = \overline{\sigma^*(\mathcal{L})}. \end{aligned}$$

It is also easy to check that $(\mathcal{L}^\vee)^\vee = \mathcal{L}$ (tensoring commutes dual), and that if \mathcal{L} is a fractional ideal, its dual is also fractional. An important fact is that an ideal and its inverse are related by multiplication with the dual ideal of the ring: for any fractional ideal \mathcal{I} , its dual ideal is $\mathcal{I}^\vee = \mathcal{I}^{-1} \cdot R^\vee$. The factor R^\vee (often called codifferent) is a fractional ideal whose inverse $(R^\vee)^{-1}$, called the different ideal, is integral and of norm $N((R^\vee)^{-1}) = \Delta_{K(T)}$, the discriminant of $K(T)$.

A.3.7 Ideal Lattice Problems

We revise here the computational problems over ideal lattices related to RLWE, and, by extension, to m -RLWE: the Shortest Vector Problem (SVP), Shortest Independent Vectors Problem (SIVP), and the Bounded Distance Decoding (BDD) Problem. The three problems can be restricted to the case of integral ideals over R (the tensor of ring of integers \mathcal{O}_{K_i}), analogously to the argument followed by Lyubashevsky *et al.* [15], [14] in the non-tensor case: if \mathcal{I} is a fractional ideal with denominator $d \in R$ (such that $d\mathcal{I} \subseteq R$ is a integral ideal), then the ideal $N(d) \cdot \mathcal{I} \subseteq R$, because $N(d) \in \langle d \rangle$.

Definition 7 (SVP and SIVP). *Let $K_{(T)}$ be a tensor number field endowed with some geometric norm (e.g, the l_2 -norm), and let $\gamma \geq 1$. The $K_{(T)}$ -SVP $_\gamma$ problem in the given norm is posed as: given a fractional ideal \mathcal{I} in $K_{(T)}$, find some nonzero $x \in \mathcal{I}$ such that $\|x\| \leq \gamma \cdot \lambda_1(\mathcal{I})$. The $K_{(T)}$ -SIVP $_\gamma$ problem is defined similarly, where the goal is to find n linearly independent elements in \mathcal{I} whose norms are all at most $\gamma \cdot \lambda_n(\mathcal{I})$.*

Definition 8 (BDD). *Let $K_{(T)}$ be a tensor number field endowed with some geometric norm (e.g, the l_2 norm), let \mathcal{I} be a fractional ideal in $K_{(T)}$, and let $d < \lambda_1(\mathcal{I})/2$. The $K_{(T)}$ -BDD $_{\mathcal{I},d}$ problem in the given norm is: given \mathcal{I} and y of the form $y = x + e$ for some $x \in \mathcal{I}$ and $\|e\| \leq d$, find x .*

A.3.8 Chinese Remainder Theorem

We reformulate the Chinese Remainder Theorem (CRT) for the ring $R = \bigotimes_{i \in [l]} \mathcal{O}_{K_i}$ in the tensor number field $K_{(T)} = \bigotimes_{i \in [l]} K_i$ and we also revisit some important concepts introduced in [14].

Lemma 9 (Chinese Remainder Theorem). *Let $\mathcal{I}_1, \dots, \mathcal{I}_r$ be pairwise coprime ideals in R , and let $\mathcal{I} = \prod_{i \in [r]} \mathcal{I}_i$. The natural ring homomorphism $R \rightarrow \bigoplus_{i \in [r]} (R/\mathcal{I}_i)$ induces a ring isomorphism $R/\mathcal{I} \rightarrow \bigoplus_{i \in [r]} (R/\mathcal{I}_i)$.*

The next lemma states that when this ring isomorphism exists, we can compute a CRT basis C for the set of pairwise coprime ideals $\mathcal{I}_1, \dots, \mathcal{I}_r$. The basis is composed by elements $c_1, \dots, c_r \in R$ that satisfy $c_i = 1 \bmod \mathcal{I}_i$ and $c_i = 0 \bmod \mathcal{I}_j$ when $i \neq j$. We can use that basis in order to invert the CRT isomorphism as follows: for any $w = (w_1, \dots, w_r) \in \bigoplus_i (R/\mathcal{I}_i)$, we have that $v = \sum_i w_i \cdot c_i \bmod \mathcal{I}$ is the unique element in R/\mathcal{I} that maps to w with that ring isomorphism.

Lemma 10 (Efficient computable basis for isomorphism). *There exists a deterministic polynomial-time algorithm that, given coprime ideals $\mathcal{I}, \mathcal{J} \subseteq R$ (represented by \mathbb{Z} -bases), outputs some $c \in \mathcal{J}$ such that $c = 1 \bmod \mathcal{I}$. More generally, there is a deterministic polynomial-time algorithm that, given pairwise coprime ideals $\mathcal{I}_1, \dots, \mathcal{I}_r$, outputs a CRT basis $c_1, \dots, c_r \in R$ for those ideals.*

Now we include two more lemmas that allow us to efficiently compute a bijection between the quotient groups $\mathcal{I}/q\mathcal{I}$ and $\mathcal{J}/q\mathcal{J}$ for any fractional ideals \mathcal{I}, \mathcal{J} . They are important for clearing out the arbitrary ideal \mathcal{I} in the BDD-to-LWE reduction. The lemmas are:

Lemma 11 (Lyubashevsky *et al.* [14] Lemma 2.14). *Let \mathcal{I} and \mathcal{J} be ideals in R . There exists $t \in \mathcal{I}$ such that the ideal $t \cdot \mathcal{I}^{-1} \subseteq R$ is coprime to \mathcal{J} . Moreover, such t can be found efficiently given \mathcal{I} and the prime ideal factorization of \mathcal{J} .*

Lemma 12 (Lyubashevsky *et al.* [14] Lemma 2.15). *Let \mathcal{I} and \mathcal{J} be ideals in R , let $t \in \mathcal{I}$ be such that $t \cdot \mathcal{I}^{-1}$ is coprime with \mathcal{J} , and let \mathcal{M} be any fractional ideal in $K_{(T)}$. Then, the function $\theta_t : K_{(T)} \rightarrow K_{(T)}$ defined as $\theta_t(u) = t \cdot u$ induces an isomorphism from $\mathcal{M}/\mathcal{J}\mathcal{M}$ to $\mathcal{I}\mathcal{M}/\mathcal{I}\mathcal{J}\mathcal{M}$, as R -modules. Moreover, this isomorphism may be efficiently inverted given $\mathcal{I}, \mathcal{J}, \mathcal{M}$ and t .*

The proof of Lemma 12 for the case where $K_{(T)}$ is a tensor of cyclotomic fields follows with the same techniques considered in [14], by taking into account that θ_t induces a homomorphism of R -modules because it represents a multiplication by a $t \in R$, so we do not include it here.

B Proof of Theorem 2

This appendix presents the proof of Theorem 2. It is based on the iterative use of the following lemma:

Lemma 13 (Extended version of Lemma 4.2 Lyubashevsky *et al.* [14]). *Let $\alpha > 0$ and $q \geq 2$ be an integer. There exists an efficient quantum algorithm that, given a fractional ideal \mathcal{I} in $K_{(T)}$, a number $r \geq \sqrt{2}q \cdot \eta_\epsilon(\mathcal{I})$ for some negligible $\epsilon = \epsilon(n)$ such that $r' = r \cdot \omega(\sqrt{\log n})/(\alpha q) > \sqrt{2n}/\lambda_1(\mathcal{I}^\vee)$, an oracle to m -R-LWE $_{q, \Psi_{\leq \alpha}}$, and a list of samples from the discrete Gaussian distribution $D_{\mathcal{I}, r}$ (as many as required by the m -R-LWE $_{q, \Psi_{\leq \alpha}}$ oracle), outputs an independent sample from $D_{\mathcal{I}, r'}$.*

Theorem 2 is proven as follows: we start with a value $r \geq 2^{2n}\lambda_n(\mathcal{I})$, in such a way that we can classically generate any polynomial number of samples from $D_{\mathcal{I}, r}$. Given the samples from $D_{\mathcal{I}, r}$, Lemma 13 can be used iteratively a polynomial number of times (using the same samples) to obtain a polynomial number of independent samples from $D_{\mathcal{I}, r'}$ with $r' = r/2$ at each iteration. Repeating this process, we can obtain samples from narrower and narrower distributions, until we have samples from a distribution with parameter $s \geq \gamma$.

Lemma 13 is obtained thanks to the following two results (Lemmas 14 and 15):

Lemma 14 (Extended version of Lemma 4.3 of Lyubashevsky *et al.* [14], proof in Section 4.2). *Let $\alpha > 0$, let $q \geq 2$ be an integer with known factorization, let \mathcal{I} be a fractional ideal in $K_{(T)}$, and let $r \geq \sqrt{2}q \cdot \eta_\epsilon(\mathcal{I})$ for some negligible $\epsilon = \epsilon(n)$. Given an oracle for the discrete Gaussian distribution $D_{\mathcal{I}, r}$, there is a probabilistic polynomial-time (classical) reduction from $BDD_{\mathcal{I}^\vee, d}$ in the l_∞ norm to m -R-LWE $_{q, \Psi_{\leq \alpha}}$, where $d = \alpha q/(\sqrt{2}r)$.*

Details for the proof of the lemma 14 follow the same steps of Lyubashevsky *et al.* for Lemma 4.3 in [14], so we do not replicate it here. However, we have to take into account that we are working with ideals over the tensor of the ring of integers, so instead of considering the lemmas 2.14 and 2.15 from [14] we have to use the redefined lemmas already presented in our work as Lemmas 11 and 12.

Lemma 15 (Extended version of Lemma 4.4 of Lyubashevsky *et al.* [14]). *There is an efficient quantum algorithm that, given any n -dimensional lattice Λ , a number $d' < \lambda_1(\Lambda^\vee)/2$ (where λ_1 is with respect to the l_2 norm), and an oracle that solves BDD on Λ^\vee except with negligible probability for points whose offset from Λ^\vee is sampled from $D_{d'/\sqrt{2n}}$, outputs a sample from $D_{\Lambda, \sqrt{n}/(\sqrt{2}d')}$. In particular, since a sample from $D_{d'/\sqrt{2n}}$ has l_∞ norm at most $d' \cdot \omega(\sqrt{\log n})/\sqrt{n}$ except with negligible probability, it suffices if the oracle solves $BDD_{\mathcal{I}^\vee, d}$ in the l_∞ norm, where $d = d' \cdot \omega(\sqrt{n})/\sqrt{n}$.*

The sketch of the proof for the lemma 13 is the following: starting with samples from $D_{\mathcal{I}, r}$ and an oracle for m -R-LWE $_{q, \Psi_{\leq \alpha}}$ and resorting to the lemma 14 we can obtain an algorithm for BDD on \mathcal{I}^\vee to within distance $d = \alpha q/(\sqrt{2}r)$ in the l_∞ norm. Next, considering Lemma 15 with $d' = d\sqrt{n}/\omega(\sqrt{\log n}) = \sqrt{n/2}/r' < \lambda_1(\mathcal{I}^\vee)/2$, we obtain a quantum procedure that outputs samples from the discrete Gaussian distribution $D_{\mathcal{I}, r'}$.

C Proofs of Theorems 3, 4 and 5

This appendix includes the proofs for the main results involving the security reductions of m -RLWE, as stated in Theorems 3, 4 and 5.

C.1 Search to Worst-Case Decision

Here we explain the two first reductions of the Theorems 3 and 4. Next, we introduce the main definitions of the intermediate problems and the corresponding lemmas, and we also highlight the differences due to working with the tensor of the rings of integers.

Definition 9 (Extended version of the \mathbf{q}_i -LWE $_{q, \Psi}$ problem, Definition 5.4 from Lyubashevsky *et al.* [14]). *The \mathbf{q}_i -LWE $_{q, \Psi}$ problem is defined as: given access to $A_{s, \psi}$ for some arbitrary $s \in R_q^\vee$ and $\psi \in \Psi$, find $s \bmod \mathbf{q}_i R^\vee$.*

Lemma 16 (LWE to \mathbf{q}_i -LWE, entending Lemma 5.5 of Lyubashevsky *et al.* [14]). *Suppose that the family Ψ is closed under all the automorphisms of $K_{(T)}$ (see Lemma 17), that is, $\psi \in \Psi$ implies that $\tau_k(\psi) \in \Psi$ for all $k \in [n]$. Then, for every $i \in [n]$, there exists a deterministic polynomial-time reduction from LWE $_{q, \Psi}$ to \mathbf{q}_i -LWE $_{q, \Psi}$.*

The proof is based on the fact that by having an oracle for \mathbf{q}_i -LWE and resorting to the different field automorphisms, we can recover s modulo $\mathbf{q}_j R^\vee$ for every $j \in [n]$ and we can use the CRT for recovering s modulo R^\vee .

The reduction works in the following way: Let $(a, b) \leftarrow A_{s, \psi}$ and apply an automorphism $(\tau_k(a), \tau_k(b))$ that satisfies $\tau_k(\mathbf{q}_j) = \mathbf{q}_i$. Now, we use the \mathbf{q}_i -LWE oracle with the transformed samples and we apply the reverse automorphism $\tau_k(t)^{-1} \in R^\vee/\mathbf{q}_j R^\vee$ to its output $t \in R^\vee/\mathbf{q}_i R^\vee$.

In order to see that $\tau_k(t)^{-1}$ has the desired value $s \bmod \mathbf{q}_j R^\vee$, we operate with the pair $(\tau_k(a), \tau_k(b))$, with $\tau_k(b) = \tau_k(a) \cdot \tau_k(s)/q + \tau_k(e) \bmod R^\vee$ where we see that the pair follows the $A_{\tau_k(s), \tau_k(\psi)}$ distribution (we know that $\tau_k(\psi) \in \Psi$, see Lemma 17). Therefore, the oracle outputs $t = \tau_k(s) \bmod \mathbf{q}_i R^\vee$ and Lemma 16 is proven.

Lemma 17 (Extended version of Lemma 5.6 of Lyubashevsky *et al.* [14]). *For any $\alpha > 0$, the family $\Psi_{\leq \alpha}$ is closed under every automorphism τ of $K_{(T)}$, that is, $\psi \in \Psi_{\leq \alpha}$ implies that $\tau(\psi) \in \Psi_{\leq \alpha}$.*

In order to see that for $\psi \in \Psi$ any possible automorphism also belongs to Ψ , we proceed as follows: each automorphism is the tensor of the existing automorphisms for each cyclotomic field, that is, $\otimes_{i \in [l]} \tau_{k_i}^{(i)}$ with $k_i \in \mathbb{Z}_{m_i}^*$. Hence, resorting to the definition of our error distributions (see Appendix A.2), we have $\psi = D_{\otimes_{i \in [l]} \mathbf{r}_i} \in \Psi_{\leq \alpha}$ where the elements of each \mathbf{r}_i are bounded by α . As the effect of the automorphism simply permutes the coordinates of each \mathbf{r}_i , we can clearly see that $\otimes_{j \in [l]} \tau_{k_j}^{(j)} \left(D_{\otimes_{i \in [l]} \mathbf{r}_i} \right) = D_{\otimes_{i \in [l]} \mathbf{r}'_i}$ for $k_j \in \mathbb{Z}_j^*$, which also belongs to $\Psi_{\leq \alpha}$ because the value of the different elements follow being at most α (they have only been permuted).

We now move on to Lemma 18 for the second reduction of the proof, but we first introduce two definitions for the intermediate problems:

Definition 10 (Extended Hybrid LWE Distribution of Lyubashvesky *et al.* [14]). *For $j \in [n]$, $s \in R_q^\vee$, and a distribution ψ over $K_{(T), \mathbb{R}}$, the distribution $A_{s, \psi}^j$ over $R_q \times \mathbb{T}$ is defined as follows: choose $(a, b) \leftarrow A_{s, \psi}$ and output $a, b + h/q$ where $h \in R_q^\vee$ is uniformly random and independent modulo $\mathfrak{q}_i R^\vee$ for all $i \leq j$, and is equal to zero modulo all the remaining $\mathfrak{q}_i R^\vee$. We also define $A_{s, \psi}^0 = A_{s, \psi}$.*

Definition 11 (Extended WDLWE $_{q, \Psi}^j$ (Worst-Case Decision LWE Relative to \mathfrak{q}_j) of Lyubashevsky *et al.* [14]). *For $j \in [n]$ and a family of distributions Ψ , the WDLWE $_{q, \Psi}^j$ problem is defined as follows: given access to $A_{s, \psi}^j$ for arbitrary $s \in R_q^\vee$, $\psi \in \Psi$, and $i \in \{j-1, j\}$, find i .*

Lemma 18 (Extended version of Search to Decision of Lyubashvesky *et al.* [14]). *For any $j \in [n]$, there exists a probabilistic polynomial-time reduction from \mathfrak{q}_j -LWE $_{q, \Psi}$ to WDLWE $_{q, \Psi}^j$.*

The proof of the reduction is based on trying each of the different possible values of s modulo $\mathfrak{q}_j R^\vee$ in such a way that after modifying the samples from $A_{q, \psi}$, we have that a) for the correct value, the samples are distributed following $A_{q, \psi}^{j-1}$ and b) for the rest of possible values, they follow $A_{q, \psi}^j$.

We can try all different values for $s \bmod \mathfrak{q}_j R^\vee$ because the norm of \mathfrak{q}_j for all j satisfies $N(\mathfrak{q}_j) = q = \text{poly}(n)$, so we can enumerate all the combinations. Finally, we can use the oracle WDLWE $_{q, \Psi}^j$ for distinguishing between the distributions $A_{q, \psi}^{j-1}$ and $A_{q, \psi}^j$.

Following an analogous procedure as the one in [14], given a sample $(a, b) \leftarrow A_{s, \psi}$, we have:

$$(a', b') = (a + v, b + (h + vg)/q) \in R_q \times \mathbb{T},$$

where $v \in R_q$ satisfies that it is uniformly random modulo \mathfrak{q}_j and zero modulo other different prime ideal, $h, g \in R_q^\vee$, where h is uniformly random and independent modulo any $\mathfrak{q}_i R^\vee$ when $i < j$, and it is zero for the rest of possible values of i . Finally, we have:

$$b' = (a's + h + v(g - s))/q + e,$$

with $e \leftarrow \psi$.

Now, choosing different values for g we have the following results: a) if $g = s \bmod \mathfrak{q}_j R^\vee$, the distribution of (a', b') is $A_{s, \psi}^{j-1}$, and b) if $g \neq s \bmod \mathfrak{q}_j R^\vee$, the distribution of (a', b') is $A_{s, \psi}^j$. Hence, we only have to enumerate different g values which satisfy different conditions modulo $\mathfrak{q}_j R^\vee$ (the values modulo other $\mathfrak{q}_i R^\vee$ with $i \neq j$ are not important) to achieve the reduction.

C.2 Worst-Case Decision to Average-Case Decision

The objective of this part is to cover the two last reductions of Theorems 3 and 4. For this purpose, we present some definitions and lemmas that allow us to reduce the worst-case decision $WDLWE_{q,\Psi}^j$ problem to an average-case problem $DLWE_{q,\Upsilon}$ where the goal is to distinguish between $A_{s,\psi}$ and uniform samples where the parameters of the error distribution are also secret and drawn from Υ .

Definition 12 (Extended version of Average-Case Decision LWE Relative to \mathbf{q}_j ($DLWE_{q,\Upsilon}^j$) of Lyubashevsky *et al.* [14]). *For $j \in [n]$ and a distribution Υ over error distributions, we say that an algorithm solves the $DLWE_{q,\Upsilon}^j$ problem if with a non negligible probability over the choice of a random $(s, \psi) \leftarrow U(R_q^\vee) \times \Upsilon$, it has a non negligible difference in acceptance probability on inputs from $A_{s,\psi}^j$ versus inputs from $A_{s,\psi}^{j-1}$.*

Lemma 19 (Extended version of Worst-Case to Average-Case Lemma 5.12 of Lyubashevsky *et al.* [14]). *For any $\alpha > 0$ and every $j \in [n]$, there is a randomized polynomial-time reduction from $WDLWE_{1,\Psi_{\leq \alpha}}^j$ to $DLWE_{q,\Upsilon_\alpha}^j$.*

In order to prove the previous lemma, let $s' \in R_q^\vee$, $\mathbf{r}' \in (\mathbb{R}^+)^n$, $k \in [n]$, and the pair (a, b) , and consider the transformation $(a, b + (a \cdot s' + h)/q + e')$ where e' is drawn from $D_{\mathbf{r}'}$, $h \in R_q^\vee$ and h satisfies that $h \bmod \mathbf{q}_i R^\vee$ are uniformly random and independent for $i \leq k$, and zero for all other i . Then, when the input is $A_{s,\psi}^j$, this transformation outputs $A_{s+s', \psi+D_{\mathbf{r}'}}^{\max\{k,j\}}$.

Now, to achieve the reduction, we repeat the following process a polynomial number of times: we draw $s' \in R_q^\vee$, and we have $\mathbf{r}' \in (\mathbb{R}^+)^n$ where $\mathbf{r}' = \bigotimes_{i \in [l]} \mathbf{r}'_i$ (as it was presented in Appendix A.2) and $r'_{i,j} = r'_{i,j+\phi(m_i)/2}$ with $i \in [l]$ and $j \in [\phi(m_i)]$. We also have $r_j'^2 = \alpha^2 \sqrt{n} x_j$ and $r_i'^2 = \alpha^2 \sqrt{n} x_i$ for all $j, i \in [n]$ and where the x_j and x_i are chosen independently from $\Gamma(2, 1)$ if r_j and r_i are different. Next, we estimate the acceptance probability of the oracle for two different input distributions: a) applying to the input the previous transformation with parameters s' , \mathbf{r}' and $j - 1$; b) applying to the input the previous transformation with parameters s' , \mathbf{r}' and j . Finally, after a polynomial number of repetitions we output $j - 1$ if there is a non negligible difference between the two acceptance probabilities; on the contrary, we output j .

Let us assume that the input distribution is $A_{q,D_{\mathbf{r}}}^{j-1}$ for some \mathbf{r} where all $r_i \in [0, \alpha]$ for $i \in [n]$. Then, we have to estimate the acceptance probability of the oracle on $A_{s+s', D_{\mathbf{r}}+D_{\mathbf{r}'}}^{j-1}$ and $A_{s+s', D_{\mathbf{r}}+D_{\mathbf{r}'}}^j$, and we notice that $D_{\mathbf{r}} + D_{\mathbf{r}'} = D_{\mathbf{r}''}$ where $r''_i = r_i'^2 + r_i^2$. If we denote by S the set of pairs (s, ψ) for which the oracle has non negligible difference in acceptance probability between $A_{q,\psi}^{j-1}$ and $A_{q,\psi}^j$, we have by assumption (the measure of S under $U(R_q^\vee) \times \Upsilon_\alpha$ is non negligible) and by claim 2 below that $(s + s', D_{\mathbf{r}} + D_{\mathbf{r}'}) \in S$ with non negligible probability, and the proof of Lemma 19 is complete.

Our Claim 2 a variant of the Claim 5.11 presented by Lyubashevsky *et al.* [14]. For our case, we need a similar result, but it must hold not only for independent variables following a $\Gamma(2, 1)$ distribution, because in our more general case, for $i \in [n]$ we can have that more than two x_i are equal. Therefore, we present a modification for vectors of coefficients distributed as $\Gamma(2, 1)$, where they do not have to be independent, and we justify its validity.

Claim 2 (Extended Claim 5.11 from [14]). *Let P be the distribution $\Gamma(2, 1)^n$ and Q be the distribution $(\Gamma(2, 1) - z_1) \times \dots \times (\Gamma(2, 1) - z_n)$ for some $0 \leq z_1, \dots, z_n \leq 1/\sqrt{n}$ where the different $\Gamma(2, 1)$ of both P and Q do not have to be independent and some of them can*

be equal to each other. Then, any set $A \subseteq \mathbb{R}^n$ whose measure under P is non negligible also has non negligible measure under Q .

The proof of the claim follows the next scheme: first, let $P, Q : \mathbb{R}^n \rightarrow \mathbb{R}^+$, where when $Q(\mathbf{x}) = 0$ we also have $P(\mathbf{x}) = 0$, and we define $R(P||Q) = \int_{\mathbb{R}^n} \frac{P(\mathbf{x})^2}{Q(\mathbf{x})} d\mathbf{x}$, considering that the fraction is zero when both the numerator and the denominator are zero. By Cauchy-Schwarz inequality, we have for any non empty set $A \subseteq \mathbb{R}^n$,

$$\frac{(\int_A P(\mathbf{x}) d\mathbf{x})^2}{\int_A Q(\mathbf{x}) d\mathbf{x}} \leq \int_A \frac{P(\mathbf{x})^2}{Q(\mathbf{x})} d\mathbf{x} \leq R(P||Q).$$

Thus, if we have a set A with non negligible measure under P and $R(P||Q) \leq \text{poly}(n)$ holds, we can say that the set A has non negligible measure under Q .

For the particular setting of the Claim 2, when $z > 0$ we have

$$R(\Gamma(2, 1)||\Gamma(2, 1) - z) = e^z \left(1 - z + z^2 e^z \int_z^\infty x^{-1} e^{-x} dx \right),$$

and when z is small, this expression reduces to $1 + z^2 \log(1/z) + \mathcal{O}(z^2)$.

The difference regarding the proof of [14] relies on the following fact: if we compute $R(P||Q)$, we have:

$$\begin{aligned} & R(\Gamma(2, 1)^n || (\Gamma(2, 1) - z_1 \times \dots \times \Gamma(2, 1) - z_n)) \\ & \leq R(\Gamma(2, 1)||\Gamma(2, 1) - z_1) \dots R(\Gamma(2, 1)||\Gamma(2, 1) - z_n), \end{aligned}$$

where the equality is achieved when all the components of each vector are independent. When some of the $\Gamma(2, 1)$ variables are equal, we can see that the ratio of the corresponding distributions is equal to the ratio of only one of the variables of P and Q respectively.

Now, as we know that the second term of the expression is bounded by $\text{poly}(n)$, the claim is proven because for the setting of the claim our expression is bounded by the second term.

Lemma 20 (Extended version of Lemma 5.14 Hybrid by Lyubashevsky *et al.* [14]). *Let Υ be a distribution over noise distributions satisfying that for any ψ in the support of Υ and any $s \in R_q^\vee$, the distribution $A_{s,\psi}^n$ is within negligible statistical distance from uniform. Then for any oracle solving the $DLWE_{q,\Upsilon}$ problem, there exists a $j \in [n]$ and an efficient algorithm that solves $DLWE_{q,\Upsilon}^j$ using the oracle.*

The proof works as follows: consider a pair (s, ψ) for which the oracle can distinguish between $A_{s,\psi}$ and uniform distribution with a non negligible advantage. By Markov's inequality, the probability measure of those pairs is non negligible. Knowing that $A_{s,\psi}^0 = A_{s,\psi}$ and that $A_{s,\psi}^n$ is negligibly far from the uniform distribution (see Lemma 21), we see that for each (s, ψ) we must have a $j \in [n]$ for which the oracle distinguishes between $A_{q,\psi}^j$ and $A_{q,\psi}^{j-1}$ with non negligible advantage. Finally, the lemma is proven if we take the j that is associated to the set of pairs (s, ψ) with the highest probability. With the proof of this lemma, the proof of the Theorem 3 is complete.

Lemma 21 (Adapted version of lemma 5.13 of Lyubashevsky *et al.* [14]). *Let $\alpha \geq \eta_\epsilon(R^\vee)/q$ for some $\epsilon > 0$. Then, for any ψ in the support of Υ_α and $s \in R_q^\vee$, the distribution $A_{s,\psi}^n$ is within statistical distance $\epsilon/2$ of the uniform distribution over (R_q, \mathbb{T}) .*

The proof of this lemma is obtained by following the steps in [14] and taking into account the considered changes in our setting together with our Lemma 5.

Finally, we introduce the needed lemma for the reductions of Theorem 4.

Lemma 22 (Extended version of Lemma 5.16 of Lyubashevsky *et al.* [14] Worst-Case to Average-Case with Spherical Noise). *For any $\alpha > 0$, $l \geq 1$, and every $j \in [n]$, there exists a randomized polynomial-time reduction from solving $WDLWE_{q, \Psi_{\leq \alpha}}^j$ to solving $DLWE_{q, D_\xi}^j$ given only l samples, where $\xi = \alpha(nl/\log(nl))^{1/4}$.*

In order to prove the Lemma 22, we consider the transformation that we have already used for the proof of the Lemma 19, but in this case the transformation has l different inputs. So, let $s' \in R_q^\vee$, $k \in [n]$, and $e_i \in \mathbb{T}$ for $i \in [l]$. Now, consider for the following l samples (a_i, b_i) the mentioned transformation $(a_i, b_i + (a_i \cdot s' + h_i)/q + e_i)$, where $h_i \in R_q^\vee$ and $i \in [l]$. It is important to note that all the h_i satisfy that they are independent and uniform modulo $q_d R^\vee$ for all $d \leq k$, and they are zero when d does not satisfy the previous relation. Therefore, if we take l independent inputs drawn from $A_{q, \psi}^j$ and we apply the transformation to all of them considering that all e_i are independently drawn from $D_{\mathbf{r}'}$, we have as output distribution $\left(A_{s+s', \psi+D_{\mathbf{r}'}}^{\max\{k, j\}}\right)^l$.

Now, the reduction repeats the following process a polynomial number of times: we consider $s' \in R_q^\vee$ and a set of independent e_i drawn from D_ξ . Next, we estimate the acceptance probability of the oracle for two different input distributions: a) applying to the input the previous transformation with parameters s' , e_i and $j-1$; b) applying to the input the previous transformation with parameters s' , e_i and j . After a polynomial number of repetitions, we output $j-1$ whenever a non negligible difference between the two acceptance probabilities is observed; otherwise, we output j .

Assuming the input distribution is $A_{s, D_{\mathbf{r}}}^{j-1}$, where all the coefficients of \mathbf{r} are in $[0, \alpha]$ for the two previous cases, we have two different output distributions: $\left(A_{s+s', \psi+D_{\mathbf{r}'}}^{j-1}\right)^l$ and $\left(A_{s+s', \psi+D_{\mathbf{r}'}}^j\right)^l$. We also consider that the coefficients of \mathbf{r}' verify $r_i'^2 = \xi^2 - r_i^2$, so we have $D_{\mathbf{r}} + D_{\mathbf{r}'} = D_\xi$.

As with Lemma 19, let S be the set of all tuples (s, e_1, \dots, e_l) for which the oracle has a non negligible difference in acceptance probability on $\left(A_{s+s', \psi+D_{\mathbf{r}'}}^{j-1}\right)^l$ and $\left(A_{s+s', \psi+D_{\mathbf{r}'}}^j\right)^l$. By our assumption and a Markov argument, the measure of S under $U(R_q^\vee) \times (D_{\mathbf{r}'})^l$ is non negligible, and we have

$$1 \leq \frac{\xi}{\sqrt{\xi^2 - r_i^2}} \leq \frac{\xi}{\sqrt{\xi^2 - \alpha^2}} \leq 1 + \sqrt{\frac{\log(nl)}{nl}},$$

where thanks to the Claim 3 below, we can assert that S is also non negligible under $U(R_q^\vee) \times (D_\xi)^l$, and where we can derive the condition $\xi = \alpha(nl/\log(nl))^{1/4}$, hence completing the proof of the Lemma 22 and the Theorem 4.

Claim 3 (Claim 5.15 from [14]). *Let $r_1, \dots, r_n \in \mathbb{R}^+$ and $s_1, \dots, s_n \in \mathbb{R}^+$ be such that for all i , $|s_i/r_i - 1| < \sqrt{(\log n)/n}$. Then any set $A \subseteq \mathbb{R}^n$ whose measure under the Gaussian distribution $D_{r_1} \times \dots \times D_{r_n}$ is non negligible, also has non negligible measure under $D_{s_1} \times \dots \times D_{s_n}$.*

References

- [1] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems. In *Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '09, pages 595–618, Berlin, Heidelberg, 2009. Springer-Verlag.

- [2] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(1):625–635, 1993.
- [3] T. Bianchi, A. Piva, and M. Barni. On the Implementation of the Discrete Fourier Transform in the Encrypted Domain. *IEEE Trans. on Information Forensics and Security*, 4(1):86–97, March 2009.
- [4] T. Bianchi, A. Piva, and M. Barni. Composite Signal Representation for Fast and Storage-Efficient Processing of Encrypted Signals. *IEEE Trans. on Information Forensics and Security*, 5(1):180–187, March 2010.
- [5] J.W. Bos, K. Lauter, J. Loftus, and M. Naehrig. Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme. In M. Stam, editor, *Cryptography and Coding*, volume 8308 of *LNCS*, pages 45–64. Springer, 2013.
- [6] Z. Brakerski. Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology CRYPTO 2012*, volume 7417 of *LNCS*, pages 868–886. Springer, 2012.
- [7] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (Leveled) Fully Homomorphic Encryption without Bootstrapping. *ACM Trans. Comput. Theory*, 6(3):13:1–13:36, July 2014.
- [8] Z. Brakerski and V. Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. In *Advances in Cryptology CRYPTO 2011*, volume 6841 of *LNCS*. Springer, 2011.
- [9] Y. Chen and P.Q. Nguyen. BKZ 2.0: Better Lattice Security Estimates. In *Advances in Cryptology ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 1–20. Springer, 2011.
- [10] J. Fan and F. Vercauteren. Somewhat Practical Fully Homomorphic Encryption. Cryptology ePrint Archive, Report 2012/144, 2012. <http://eprint.iacr.org/>.
- [11] Roger A. Horn and Charles R. Johnson. *Topics in Matrix Analysis*. Cambridge University Press, 1991. Cambridge Books Online.
- [12] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications*. Cambridge university press, 1994.
- [13] R. Lindner and C. Peikert. Better Key Sizes (and Attacks) for LWE-based Encryption. In *CT-RSA ’11*, pages 319–339. Springer, 2011.
- [14] V. Lyubashevsky, C. Peikert, and O. Regev. On Ideal Lattices and Learning with Errors over Rings. *J. ACM*, 60(6):43:1–43:35, November 2013.
- [15] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. *Advances in Cryptology – EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 – June 3, 2010. Proceedings*, chapter On Ideal Lattices and Learning with Errors over Rings, pages 1–23. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.
- [16] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. *Advances in Cryptology – EUROCRYPT 2013: 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, chapter A Toolkit for Ring-LWE Cryptography, pages 35–54. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

- [17] Léo Ducas Martin Albrecht, Shi Bai. A subfield lattice attack on overstretched NTRU assumptions: Cryptanalysis of some FHE and Graded Encoding Schemes. Cryptology ePrint Archive, Report 2016/127, 2016. <http://eprint.iacr.org/2016/127>.
- [18] D. Micciancio and O. Regev. Lattice-based Cryptography. In *Post-Quantum Cryptography*, pages 147–191. Springer, 2009.
- [19] Daniele Micciancio and Oded Regev. Worst-Case to Average-Case Reductions Based on Gaussian Measures. *SIAM J. Comput.*, 37(1):267–302, April 2007.
- [20] P. Paillier. Public-key Cryptosystems Based on Composite Degree Residuosity Classes. In *EUROCRYPT’99*, pages 223–238. Springer, 1999.
- [21] A. Pedrouzo-Ulloa, J.R. Troncoso-Pastoriza, and F. Pérez-González. Multivariate Lattices for Encrypted Image Processing. In *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1707–1711, April 2015.
- [22] Alberto Pedrouzo-Ulloa, Juan Ramón Troncoso-Pastoriza, and Fernando Pérez-González. Number Theoretic Transforms for Secure Signal Processing. *IEEE Trans. on Information Forensics and Security* (submitted).
- [23] Chris Peikert and Alon Rosen. Lattices that admit logarithmic worst-case to average-case connection factors. In *Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing, STOC ’07*, pages 478–487, New York, NY, USA, 2007. ACM.
- [24] Oded Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *J. ACM*, 56(6):34:1–34:40, September 2009.
- [25] Jean-Pierre Serre. *Linear Representations of Finite Groups*. Springer-Verlag New York, 1977.
- [26] J.R. Troncoso-Pastoriza, D. Gonzalez-Jimenez, and F. Perez-Gonzalez. Fully Private Noninteractive Face Verification. *IEEE Trans. on Information Forensics and Security*, 8(7):1101–1114, July 2013.
- [27] J.R. Troncoso-Pastoriza, S. Katzenbeisser, M. Celik, and A. Lemma. A Secure Multidimensional Point Inclusion Protocol. In *9th ACM Workshop on Multimedia & Security*, pages 109–120, 2007.